KPB.410.004.05.2015
Nr ewid. 42/2016/P/15/042/KPB

Informacja o wynikach kontroli

ZAPEWNIENIE BEZPIECZEŃSTWA DZIAŁANIA SYSTEMÓW INFORMATYCZNYCH WYKORZYSTYWANYCH DO REALIZACJI ZADAŃ PUBLICZNYCH

DEPARTAMENT PORZĄDKU
I BEZPIECZEŃSTWA WEWNĘTRZNEGO

MISJĄ

Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ

Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Dyrektor Departamentu Porządku
i Bezpieczeństwa Wewnętrznego:
Marek Bieńkowski

Zatwierdzam:
Krzysztof Kwiatkowski

Prezes Najwyższej Izby Kontroli
Warszawa, dnia 14.04.2016 r.

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

Spis treści

Wykaz stosowanych skrótów, skrótowców i pojęć

Akceptowane ryzyka	Ogłoszona decyzja o podjęciu określonego ryzyka; akceptowane ryzyka podlegają monitorowaniu i przeglądowi.
Aktywa	Wszystko, co dla instytucji stanowi wartość.
Analiza ryzyka	Proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka.
Autentyczność	Właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane.
Bezpieczeństwo informacji	Zachowanie poufności, integralności i dostępności informacji.
COBIT	Control Objectives for Information and related Technology – zbiór dobrych praktyk pomagający optymalizować inwestycje związane z technologiami informatycznymi (IT) i zapewniać dostępność usług oraz dostarczający mierników i modeli dojrzałości umożliwiających ocenę wyników procesów IT i określenie odpowiednich obowiązków właścicieli procesów biznesowych i IT. W niniejszej kontroli wykorzystano przetłumaczoną na język polski wersję 4.1 tego standardu.
Cyberprzestrzeń	Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[1], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
Dostępność	Cecha bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu.
Incydent związany z bezpieczeństwem informacji (incydent bezpieczeństwa)	Pojedyncze, niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Integralność	Właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.
IT	Technologia informacyjna, stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane ze zbieraniem, przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji.
Kontrola dostępu	Środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa.
KRI	Krajowe Ramy Interoperacyjności – stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą.

[1] Dz. U z 2014 r. poz. 1114.

Kryteria ryzyka Poziomy odniesienia, względem których określa się ważność ryzyka.

Model dojrzałości Stosowana w metodyce Cobit 4.1 metoda oceny zarządzania i sprawowania kontroli nad procesami IT. Stopień dojrzałości organizacji może być oceniony w skali od 0 (brak) do 5 (optymalna).

Ocena ryzyka Proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane.

Polityka Zamierzenia i kierunek organizacji formalnie wyrażone przez jego kierownictwo.

Poufność Właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom.

Poziom ryzyka Wielkość ryzyka wyrażona w kategoriach kombinacji następstw oraz ich prawdopodobieństw.

Przegląd Działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności w dziedzinie osiągania ustalonych celów.

Rozporządzenie KRI Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[2].

Ryzyko Wpływ niepewności na cele. Następstwem jest odchylenie od oczekiwań, które może być pozytywne lub negatywne. Niepewność to stan, również częściowy, niedoboru informacji związanej ze zrozumieniem lub wiedzą na temat zdarzenia jego następstw lub prawdopodobieństwa jego wystąpienia.

SZBI System Zarządzania Bezpieczeństwem Informacji.

Szacowanie ryzyka Całościowy proces wyszukiwania, rozpoznawania i opisywania ryzyka, poznania jego charakteru oraz określenia poziomu zakończony analizą ryzyka i porównywaniem wyników z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub mogą być tolerowane.

Uwierzytelnienie Pewność, że deklarowana charakterystyka podmiotu jest poprawna.

Właściciel ryzyka Osoba lub podmiot odpowiedzialne za zarządzanie ryzykiem i uprawniony do zarządzania nim.

Zabezpieczenie Środek, który modyfikuje ryzyko. Zabezpieczenia obejmują procesy, politykę, urządzenia, praktyki lub inne działania modyfikujące ryzyko. Zabezpieczenia nie zawsze wywierają zamierzony lub zakładany wpływ.

Zdarzenie związane z bezpieczeństwem informacji Stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

---

[2] Dz. U. z 2016 r. poz. 113.

WPROWADZENIE

Sprawna realizacja coraz większej liczby zadań postawionych przed administracją państwa związana jest z koniecznością wykorzystania nowoczesnych technologii. Instytucje realizujące zadania publiczne aktualnie korzystają z szeregu różnych, często bardzo skomplikowanych, systemów teleinformatycznych. Coraz więcej istotnych informacji dotyczących funkcjonowania państwa i życia jego obywateli jest gromadzonych na nośnikach cyfrowych i przetwarzanych w systemach administrowanych przez organy państwowe. Dane te na szeroką skalę są zbierane, przechowywane, modyfikowane, przesyłane i usuwane. Zapewnienie im odpowiedniego poziomu bezpieczeństwa, w tym zabezpieczenie przed kradzieżą, utratą, nieuprawnioną modyfikacją, wymaga podjęcia wielokierunkowych działań, także odpowiedniego sprzętu, oprogramowania, środków łączności, personelu oraz organizacji.

Wśród przekazywanych przez media informacji wskazuje się coraz częściej na nowe zagrożenia dotyczące nie tylko komputerów prywatnych, ale również będących w dyspozycji instytucji publicznych, które w ostatnim okresie niejednokrotnie poniosły wymierne straty związane z przestępstwami dokonanymi za pomocą narzędzi i metod informatycznych.

Przeprowadzona w 2015 r. przez NIK kontrola pt. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* wykazała, że administracja państwowa nie podjęła dotychczas działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski. Stwierdzono, że działania podmiotów publicznych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez wizji systemowej. Kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji publicznej. W rezultacie stwierdzono brak spójnych i systemowych działań mających na celu monitorowanie, przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni RP oraz minimalizowanie skutków ewentualnych incydentów. Spowodowane to było brakiem:

- narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne;
- struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, definicji obowiązków i uprawnień jego uczestników oraz przydzielenia zasobów niezbędnych do skutecznej realizacji zadań;
- procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią.

Powyższe, alarmujące ustalenia, odnoszące się do poziomu strategicznego, wywołały pytania na temat tego jak w sytuacji braku centralnych rozwiązań zapewniane są warunki bezpieczeństwa konkretnych, istotnych dla funkcjonowania państwa systemów informatycznych.

W związku z powyższym, w ramach niniejszej kontroli NIK podjęła próbę szczegółowego zbadania czy instytucje administrujące systemami informatycznymi służącymi do realizacji istotnych zadań publicznych zapewniają warunki dla bezpiecznego ich działania. Istotnym było również zbadanie, w jakim stopniu organy państwa zabezpieczają dane, którymi administrują.

1 ZAŁOŻENIA KONTROLI

Kontrola planowa nr P/15/042 – *Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych.*

Cel główny kontroli

Ocena czy w kontrolowanych jednostkach zapewnione jest bezpieczeństwo danych gromadzonych w systemach przeznaczonych do realizacji istotnych zadań publicznych.

Cele cząstkowe

Cele cząstkowe zostały podzielone na dwa obszary poddane ocenie, w ramach których dążono do uzyskania odpowiedzi na pytania szczegółowe.

1) W obszarze wspierania bezpieczeństwa IT na poziomie całej organizacji badano czy:
   – prowadzone jest zarządzanie bezpieczeństwem IT,
   – wdrożono plany zapewnienia bezpieczeństwa IT,
   – testuje się, nadzoruje i monitoruje bezpieczeństwo IT,
   – zdefiniowano incydenty związane z bezpieczeństwem IT,
   – zarządza się kluczami kryptograficznymi,
   – wdrożono ochronę przed złośliwym oprogramowaniem, jego wykrywanie i dystrybucję poprawek,
   – zapewniono bezpieczeństwo sieciowe.
2) W obszarze wspierania bezpieczeństwa na poziomie wybranego systemu badano czy:
   – zarządza się tożsamościami i kontami użytkowników,
   – chroni się technologie zabezpieczeń i wrażliwe dane.

Podstawa prawna, kryteria i przyjęta metodyka oceny kontrolowanej działalności

Kontrolę przeprowadzono na podstawie art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3] (ustawa o NIK), zgodnie z kryteriami określonymi w art. 5 ust. 1 ustawy, tj. legalności, gospodarności, celowości i rzetelności.

Wobec braku centralnych zaleceń i wymagań dotyczących bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych NIK przyjęła jako wyznaczniki służące ocenie kontrolowanej działalności wskazania wynikające z Polskich Norm[4], literatury fachowej i dobrych praktyk dotyczących tego obszaru oraz minimalne wymagania dla systemów teleinformatycznych zawarte w rozporządzeniu KRI. Przedmiotem kontroli nie było jednak weryfikowanie zastosowanych dla zapewnienia bezpieczeństwa rozwiązań technicznych, ale ocena warunków i podstaw, w szczególności formalnych, stworzonych w celu zapewnienia tego bezpieczeństwa.

W związku ze złożoną tematyką oraz brakiem szczegółowych regulacji prawnych dot. kontrolowanej działalności, a w szczególności w celu obiektywnej i jednorodnej oceny poziomu zarządzania procesami zapewnienia bezpieczeństwa poszczególnych systemów teleinformatycznych, zastosowano model ocen opisowych opierający się na stosowanym w metodyce COBIT modelu dojrzałości. [szerzej o tej metodyce str. 22–23 Informacji]

3 Dz. U. z 2015 r. poz. 1096.

4 PN-ISO/IEC 27001:2007.

Badania kontrolne objęły swym zakresem główne elementy systemu bezpieczeństwa informacji, tj. obszary ze sfery: planuj, wykonaj, sprawdzaj, doskonal[5] (obszary te, wraz z powiązaniami między nimi, przedstawiają diagramy zawarte na str. 39–41 Informacji).

Zakres podmiotowy i przedmiotowy kontroli

Kontrolą objęto sześć wybranych instytucji realizujących ważne zadania publiczne, tj. Ministerstwo Skarbu Państwa, Ministerstwo Spraw Wewnętrznych, Ministerstwo Sprawiedliwości, Komendę Główną Straży Granicznej, Narodowy Fundusz Zdrowia oraz Kasę Rolniczego Ubezpieczenia Rolniczego[6].

W każdej z powyższych instytucji wybrano po analizie jeden z istotnych systemów informatycznych i objęto go szczegółowym badaniem.

Wykaz kontrolowanych podmiotów i wybranych do badań kontrolnych systemów informatycznych przedstawia poniższa tabela.

Tabela nr 1

Jednostka	System objęty badaniem	Zadania publiczne realizowane za pomocą systemu
Ministerstwo Skarbu Państwa (MSP)	Zintegrowany System Informatyczny (ZSI)	Podstawowym systemem informatycznym, który wspomaga funkcjonowanie ministerstwa (księgowość, kadry, rachuba płac, itd.) oraz obsługuje ustawowe zadania MSP (gospodarowanie mieniem SP, komercjalizacja i prywatyzacja itd.).
Ministerstwo Spraw Wewnętrznych	Centralna ewidencja wydanych i unieważnionych dokumentów paszportowych (CEWiUDP)	System obsługujący wydawanie paszportów przez urzędy wojewódzkie oraz umożliwia pogląd do danych paszportowych przez upoważnione służby.
Ministerstwo Sprawiedliwości	Nowa Księga Wieczysta (NKW)	System umożliwiający gromadzenie, przetwarzanie i udostępnianie informacji zawartych w księgach wieczystych (m.in. dane o właścicielu i stanie prawnym nieruchomości).
Komenda Główna Straży Granicznej	Centralna Baza Danych Straży Granicznej (SI NKW)	System którego jednym z podstawowych zadań jest wspomaganie realizacji podstawowych, statutowych zadań, nałożonych na Straż Graniczną przepisami prawa polskiego lub umowami międzynarodowymi w zakresie odprawy granicznej i kontroli realizowanych przez funkcjonariuszy SG.
Narodowy Fundusz Zdrowia	Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców (eWUŚ)	System pozwalający szerokorozumianej służbie zdrowia na weryfikację posiadanych przez pacjenta praw do świadczeń opieki zdrowotnej.
Kasa Rolniczego Ubezpieczenia Rolniczego	FARMER	System informatyczny wspomagający wypłatę świadczeń emerytalno-rentowych dla rolników . W chwili obecnej wspomaga wypłatę dla ok. 1,5 mln świadczeniobiorców.

Okres objęty kontrolą

Kontrolą objęto okres od 1 stycznia 2014 r. do 1 października 2015 r.

[5] Taki, znany model – „Planuj – Wykonuj – Sprawdzaj – Działaj" (PDCA) stosuje Norma PN-ISO/IEC 27001. Jest on stosowany do całej struktury procesów SZBI. Proces wdrażania SZBI został w taki sposób zdefiniowany.

[6] Ta ostatnia jednostka posiada aktualny certyfikat ISO w zakresie zapewnienia bezpieczeństwa informacji.

2 PODSUMOWANIE WYNIKÓW KONTROLI

2.1 Ogólna ocena kontrolowanej działalności

W ocenie Najwyższej Izby Kontroli, stopień przygotowania oraz wdrożenia Systemu Zapewnienia Bezpieczeństwa Informacji nie zapewniał akceptowalnego[7] poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych.

Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny. Spośród sześciu skontrolowanych jednostek tylko KRUS wdrożyła Systemu Zapewnienia Bezpieczeństwa Informacji (SZBI), chociaż należy zauważyć, iż jego funkcjonowanie było również obarczone istotnymi nieprawidłowościami. W większości zbadanych jednostek (wszystkich poza KRUS) prace nad zapewnieniem odpowiednich warunków bezpieczeństwa informacji przetwarzanych w systemach informatycznych nie osiągnęły właściwego poziomu – zostały niedawno rozpoczęte i znajdują się na wstępnym etapie, obejmującym opracowanie niezbędnych podstaw formalnych – polityk bezpieczeństwa i powiązanych z nimi szczegółowych procedur.

W związku z powyższym, w skontrolowanych podmiotach (z wyjątkiem KRUS) **opierano się na uproszczonych lub nieformalnych zasadach wynikających z dobrych praktyk lub dotychczasowych doświadczeń pracowników działów IT**. Zdaniem NIK, **takie doraźne działania nie zapewniały adekwatnego do zagrożeń zarządzania bezpieczeństwem danych.** Kontrola wykazała w tym obszarze **braki dotyczące m.in.**: wadliwych planów zapewnienia bezpieczeństwa oraz ograniczonego zakresu nadzoru, testowania i monitorowania bezpieczeństwa. **Zgodnie z metodologią Cobit 4.1, poziom zarządzania procesem zapewnienia bezpieczeństwa w poszczególnych kontrolowanych jednostkach wahał się pomiędzy „początkowy/doraźny" (1) a „zdefiniowanym" (3),** w skali od zera do pięciu, gdzie pięć stanowi wartość maksymalną.

Główny ciężar zapewnienia bezpieczeństwa IT w kontrolowanych jednostkach spoczywał na koordynatorze ds. bezpieczeństwa, który jednak nie posiadał w praktyce kompetencji w zakresie zarządzania całym procesem. Często też zadania te były realizowane jednoosobowo. Powoływano wprawdzie zespoły specjalistów lub zawierano umowy z wykonawcami zewnętrznymi, jednakże nie sporządzano niezbędnych analiz, czy usługi świadczone przez nich zaspakajają potrzeby jednostki w zakresie bezpieczeństwa.

Świadomość potrzeby zapewnienia bezpieczeństwa informatycznego była w kontrolowanych jednostkach fragmentaryczna i ograniczona. Chociaż same systemy informatyczne oraz przeprowadzane audyty dostarczały informacji dotyczących stanu bezpieczeństwa, to dane te nie były odpowiednio analizowane i wykorzystywane. Bezpieczeństwo danych było postrzegane głównie jako przedmiot odpowiedzialności i domena działu IT, a nie wszystkich komórek realizujących zadania statutowe, co w dużej mierze utrudniało wypracowanie spójnych dla całej instytucji systemów zarządzania bezpieczeństwem informatycznym. Wprawdzie polityka dotycząca bezpieczeństwa była cały czas rozwijana, to jednak nie towarzyszyły jej adekwatne umiejętności pracowników i rozwój narzędzi niezbędnych do jej realizacji. We wszystkich jednostkach sprawozdawczość dotycząca bezpieczeństwa IT była niekompletna, nierzetelna, a w niektórych przypadkach obarczona błędami.

---

[7] W przypadku systemów IT, ze względu na szybki rozwój technologii, nie można mówić o zapewnieniu pełnego bezpieczeństwa. Celem podmiotów publicznych powinno być natomiast dążenie do minimalizacji ryzyka utraty danych lub zakłócenia funkcjonowania systemów IT do poziomu akceptowalnego, który to poziom powinien być indywidualnie określany dla poszczególnych systemów.

Porównując jakość realizacji obowiązków dotyczących zapewnienia bezpieczeństwa informacji z punktu widzenia całych organizacji i wybranych systemów stwierdzić należy, że w tym drugim obszarze realizacja zadań była na nieco wyższym poziomie. W ocenie NIK może to wynikać z wpływu, jaki na zapewnienie bezpieczeństwa miała praktyczna wiedza i zaangażowanie średniego personelu technicznego oraz z coraz powszechniejszego wykorzystywania w administracji państwowej komercyjnych systemów informatycznych, opartych o standardowe na rynku, nowoczesne rozwiązania wspierające zapewnianie bezpieczeństwa. Dzięki wykorzystaniu tych rozwiązań oraz dotychczasowych doświadczeń i dobrych praktyk, możliwe było utrzymywanie pewnego poziomu bezpieczeństwa funkcjonowania poszczególnych systemów w warunkach ograniczonych zasobów, braków organizacyjnych lub niefunkcjonujących regulacji, jednakże w ocenie NIK nie jest to stan, który powinien być traktowany jako skuteczne rozwiązanie docelowe. **W dobie bowiem dynamicznego wzrostu zagrożeń zapewnienie bezpieczeństwa systemów IT nie może być oparte na chaotycznie zarządzanych, ukierunkowanych jedynie na przezwyciężanie aktualnych trudności, działaniach.**

Źródło: Fotolia.com.

2.2 Synteza wyników kontroli

System zarządzania bezpieczeństwem informacji

Podmiot realizujący zadania publiczne, zgodnie z § 20 ust. 1 rozporządzenia KRI[8], opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[9].

Spośród sześciu skontrolowanych podmiotów, KRUS był jedyną, w której formalnie wdrożono System Zarządzania Bezpieczeństwem Informacji.

[8] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. z 2016 r. poz. 113).

[9] Kwestie te zostały szczegółowo omówione w pkt 3.1.2 Organizacja bezpieczeństwa informacji, str. 16 i n.

W pozostałych zbadanych jednostkach prace nad zapewnieniem odpowiednich warunków bezpieczeństwa informacji przetwarzanych w systemach informatycznych nie osiągnęły właściwego poziomu – zostały niedawno rozpoczęte i znajdują się na wstępnym etapie, obejmującym opracowanie niezbędnych podstaw formalnych – polityk bezpieczeństwa i powiązanych z nimi szczegółowych procedur. Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i praktycznie – wobec braku procedur – intuicyjny. W podmiotach tych **opierano się na uproszczonych lub nieformalnych zasadach wynikających z dobrych praktyk lub doświadczenia pracowników działów IT**. Zdaniem NIK **takie doraźne działania nie zapewniały odpowiedniego, bezpiecznego i spójnego zarządzania bezpieczeństwem danych.** Kontrola wykazała w tym obszarze **braki dotyczące m.in.**: wadliwych planów zapewnienia bezpieczeństwa oraz ograniczonego zakresu nadzoru, testowania i monitorowania bezpieczeństwa. **Zgodnie z metodologią Cobit 4.1 poziom zarządzania procesem zapewnienia bezpieczeństwa w kontrolowanych jednostkach, mierzony w skali od zera do pięciu, można określić jako:**

- **„zdefiniowany" (poziom trzeci) – KRUS;**
- **„powtarzalny lecz intuicyjny" (poziom drugi) – Ministerstwo Sprawiedliwości, Ministerstwo Skarbu Państwa, Narodowy Fundusz Zdrowia;**
- **„początkowy/doraźny" (poziom pierwszy) – Ministerstwo Spraw Wewnętrznych i Straż Graniczna.**

Kontrola zidentyfikowała w KRUS w**prowadzenie praktycznie wszystkich procesów wymaganych przez przyjętą metodykę badań, czego nie stwierdzono w żadnej z pozostałych kontrolowanych jednostek**. Było to związane z działaniami podjętymi w celu uzyskania przez KRUS certyfikatu ISO 27001. Porównując wyniki kontroli dla wszystkich skontrolowanych jednostek, zarówno posiadających jak i nieposiadających ww. certyfikat, należy wskazać na **pozytywny wpływ wymagań procesu certyfikacji na uzyskaną ocenę warunków zapewnienia bezpieczeństwa IT**. W konsekwencji ocena sformułowana dla KRUS była wyraźnie wyższa niż dla pozostałych jednostek.

[szerzej str. 30 Informacji]

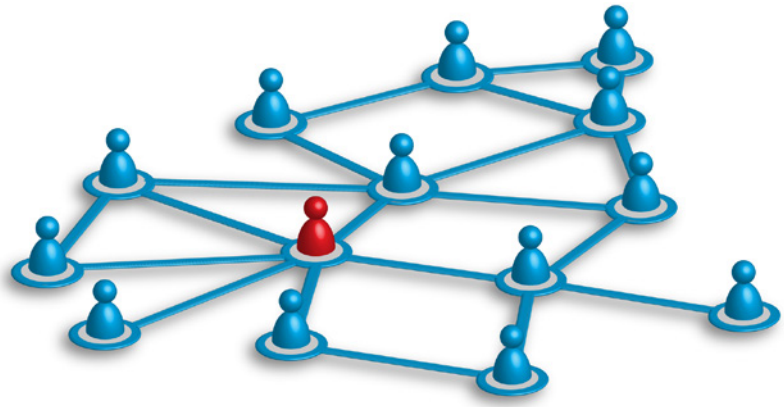
Źródło: Fotolia.com.

Jednakże również w systemie funkcjonującym w KRUS kontrola wykryła nieprawidłowości. Wskazywały one na **występowanie błędów w implementacji wymagań norm stanowiących podstawę uzyskania certyfikatu**. W ocenie NIK niektóre z nich były poważne i mogą mieć istotny, negatywny wpływ na szereg procesów zapewnienia bezpieczeństwa IT w KRUS. Stwierdzone nieprawidłowości dotyczyły rozbieżności pomiędzy deklarowanym a faktycznym poziomem zabezpieczenia informacji. Był to niepokojący stan, zwłaszcza że **podmioty które zorganizowały**

swój system zarządzania bezpieczeństwem informacji, ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie na podstawie Polskich Norm zostały praktycznie zwolnione z przestrzegania szeregu wymagań rozporządzenia KRI. Wymagania wskazane w Normie są znacznie szersze i precyzyjniejsze niż w rozporządzeniu, jednak stwierdzona w KRUS rozbieżność wskazywała na istnienie ryzyka niespełniania wymogów określonych w rozporządzeniu. **Niezależnie od powyższego stwierdzić należy, że System Zarządzania Bezpieczeństwem Informacji w KRUS funkcjonował, chociaż występowały w nim istotne nieprawidłowości.** Przykładowo w odniesieniu do głównych procedur bezpieczeństwa Izba wniosła szereg uwag do ich czytelności i kompletności. Przyjęta koncepcja powierzenia zasobów KRUS wykonawcy zewnętrznemu, m.in. w zakresie systemów służących realizacji podstawowych ustawowych zadań nie została poprzedzona stosowymi analizami – m.in. nie określono sposobu szacowania ryzyka związanego z utratą informacji w sytuacji powierzenia zasobów firmie zewnętrznej. Co za tym idzie, nie zapewniono odpowiednich zasobów (przede wszystkim kadrowych[10]) oraz nie wypracowano realnych narzędzi nadzoru nad bezpieczeństwem informacji przekazanych podmiotom zewnętrznym W stworzonym w KRUS systemie zarządzania bezpieczeństwem informacji określonym celom w zakresie bezpieczeństwa nie przypisano miernika, oraz zasobów niezbędnych do ich osiągnięcia. System zbierania i analizy incydentów był niekompletny, tj. nie obejmował m.in. incydentów obsługiwanych przez administratorów oraz incydentów systemu FARMER. [szerzej str. 21 i n. oraz 30 i n. Informacji]

Identyfikacja ryzyka

Kontrolowane jednostki w ograniczonym zakresie wykorzystywały metody identyfikacji, monitorowania i zapobiegania ryzyku związanemu z bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych. W niektórych jednostkach proces ten był związany jedynie z realizacją wymagań Polityki Ochrony Cyberprzestrzeni[11], przepisów o ochronie informacji niejawnych lub obowiązków związanych z operowaniem infrastrukturą krytyczną.



Źródło: Fotolia.com.

Zdaniem NIK te wycinkowe działania nie mogły zastąpić odpowiednio przygotowanego procesu szacowania ryzyka przeprowadzonego w odniesieniu do wszystkich posiadanych i przetwarzanych informacji, z uwzględnieniem realizowanych zadań i specyfiki instytucji. Rzetelne przeprowadzenie procesu szacowania ryzyka powinno być poprzedzone m.in. doborem metodyki prac, zidentyfikowaniem

[10] Według ustaleń kontroli minimalny zespół zajmujący się nadzorem nad realizacją umowy przez wykonawcę powinien liczyć 3 osoby, gdy tymczasem czynności wykonywał jeden pracownik, któremu powierzono również inne zadania.

[11] Strategiczny dokument przyjęty na podstawie uchwały Rady Ministrów z dnia 25 czerwca 2013 r., którego celem jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa.

aktywów i określeniem ich wartości. Przygotowanie tych danych wejściowych ma w tym kontekście zasadnicze znaczenie dla identyfikowania obszarów z jednej strony „najcenniejszych" dla jednostki, a z drugiej strony najbardziej zagrożonych. W sytuacji ograniczonych zasobów przeznaczanych na bezpieczeństwo systemów IT szacowanie ryzyka oraz kosztów niezbędnych celem jego ograniczenia powinno być podstawowym zadaniem osób odpowiedzialnych za ich bezpieczeństwo.

Braki w powyższym zakresie, stanowiącym dane wejściowe do budowy systemu bezpieczeństwa informacji, w skład których wchodzą wykazy aktywów oraz wyniki szacowania ryzyka powodowało, że **środki wydawane na bezpieczeństwo informacji przeznaczane były na realizację poszczególnych zadań w sposób intuicyjny**.

Zabezpieczenie informacji mających podstawowe znaczenie dla kontrolowanych jednostek

Istniała **duża dysproporcja pomiędzy działaniami podejmowanymi dla ochrony poszczególnych grup informacji, tj. informacji objętych ustawową ochroną (niejawnych i danych osobowych) oraz innych informacji, których ochrona nie została wprost usankcjonowana, ale które stanowią dużą wartość dla poszczególnych jednostek**, czasem będąc nawet podstawą ich funkcjonowania. Zdaniem NIK ten stan może oznaczać, że:

- uzyskanie odpowiedniego poziomu ochrony informacji następuje w konsekwencji funkcjonowania konkretnych (dotyczących w tym przypadku informacji niejawnych lub danych osobowych) przepisów prawa, które w szczegółowy sposób określają metody zapewnienia bezpieczeństwa, procedury postępowania, wymagania dla sprzętu i użytkowników, wskazują organy uprawnione do kontroli oraz, co istotne, penalizują ewentualne błędy, pomyłki i naruszenia;
- w jednostkach kontrolowanych brak było świadomości, że oprócz informacji, których szczegółowy wymóg ochrony zapisany jest w przepisach prawa istnieją także inne informacje, równie ważne, o których ochronę każda jednostka powinna zadbać samodzielnie.

W porównaniu do normatywnie określonych wymogów dla ochrony informacji niejawnych i danych osobowych, zidentyfikowanie wszelkich innych, istotnych informacji oraz wybór metod ich chronienia jest praktycznie pozostawiony w gestii ich posiadacza. Prowadzi to do sytuacji, w których **instytucje, po przeanalizowaniu aktualnie funkcjonujących przepisów nie widzą konieczności podejmowania innych działań związanych z bezpieczeństwem informacji, niż zapisanych w ustawie o ochronie informacji niejawnych oraz ustawie o ochronie danych osobowych**.

Zdaniem NIK stwierdzona w trakcie kontroli praktyka ograniczania ochrony do jedynie niektórych istotnych informacji może mieć poważne konsekwencje dla właściwego szacowania ryzyka, dzielenia zasobów, oraz zapewnienia ciągłości działania instytucji mających istotne znaczenie dla funkcjonowania państwa.

Źródło: Fotolia.com.

Odpowiedzialność za bezpieczeństwo danych

W większości kontrolowanych jednostek **zagadnienia dotyczące bezpieczeństwa informacji znajdowały się w gestii komórek bezpośrednio odpowiedzialnych za systemy informatyczne**. Zdaniem NIK powodowało to **ograniczenie faktycznego zakresu ochrony informacji jedynie do systemów informatycznych i nośników danych**. Podejście to zawężało, z przyczyn kompetencyjnych, możliwości budowania systemów ochrony informacji obejmujących całe instytucje oraz mogło zmniejszać wielkość zasobów angażowanych w ochronę informacji. Zdaniem NIK taki model organizacyjny powodował, że pozostałe komórki organizacyjne nie czując się współodpowiedzialnymi za ochronę informacji, uznały jej wymagania jako nieuzasadnione utrudnienia wynikające jedynie ze specyfiki pracy informatyków. W konsekwencji powyższego również **kierownictwa tych instytucji, niejako „przekazując problem do rozwiązania" specjalistycznej komórce, w niedostatecznym zakresie uznawały swoją rolę w kreowaniu i osiąganiu strategicznych celów dotyczących bezpieczeństwa informacji**.

Odpowiedzialność za zapewnienie bezpieczeństwa informacji powierzano przede wszystkim Koordynatorowi ds. tego bezpieczeństwa (często było to stanowisko jednoosobowe), który nie posiadał dostatecznych uprawnień i możliwości do działania w sferze zarządzania procesem i skoordynowania działań związanych z zapewnieniem bezpieczeństwa w skali całej jednostki.

Źródło: Fotolia.com.

Audyty bezpieczeństwa

Kontrola wykazała **pozytywny wpływ audytów związanych z bezpieczeństwem informacji** wykonywanych doraźnie, z inicjatywy własnej lub corocznie, w związku z realizacją norm rozporządzenia KRI. Raporty z tych audytów stanowiły w praktyce dla kierownictw kontrolowanych jednostek **jedyne istotne źródło informacji o realnym stanie bezpieczeństwa, różnych aspektach jego utrzymania oraz działaniach niezbędnych do przeprowadzenia**. Ustalony w kilku jednostkach stan dynamicznego wzrostu zainteresowania ich kierownictw jakością wykorzystywanych polityk bezpieczeństwa i towarzyszących im dokumentów, wdrażaniem Systemów Zapewnienia Bezpieczeństwa Informacji oraz modyfikowaniem struktur odpowiedzialnych za bezpieczeństwo, wynikał bezpośrednio z otrzymanych raportów, m.in. obowiązkowych audytów wynikających z realizacji rozporządzenia KRI.

W ocenie Izby prowadzenie przedmiotowych audytów w istotny sposób wpłynęło na świadomość potrzeb zapewnienia bezpieczeństwa IT. **Negatywnie należy jednak ocenić fakt, że problematyka takiego bezpieczeństwa zyskała na znaczeniu dopiero w ostatnim okresie**[12].

Istotnym problemem był brak konsekwencji i zaangażowania kierownictw kontrolowanych jednostek w realizację zaleceń audytorów. W tym zakresie ocena wynikająca z ustaleń przeprowadzonej kontroli była zdecydowanie niższa. **Większość podjętych interwencyjnie działań mających poprawić stan bezpieczeństwa IT utraciło początkowy impet, powołane zespoły specjalistyczne zbierały się nieregularnie, przygotowywanie nowych regulacji przebiegało opieszale, co przy ograniczonych zasobach wymuszało w praktyce powrót do realizacji jedynie rutynowych zadań**.

Źródło: Fotolia.com.

Odrębnym zagadnieniem, budzącym znaczne kontrowersje, jest problematyka jawności dokumentów wytworzonych w trakcie prowadzonych audytów. Problemem dotyczył klasyfikowania dokumentów i polegał na nadawaniu klauzul niejawności dokumentom wytworzonym w trakcie audytów bezpieczeństwa informacji. Zgodnie z wyrokiem Trybunału Konstytucyjnego[13] władze publiczne powinny udostępniać takie dokumenty każdej osobie, która o to poprosi, traktując je jako informację publiczną. Jednostki kontrolowane wskazywały natomiast na potencjalne zagrożenia związane z publikacją informacji dotyczących funkcjonujących systemów, w szczególności ich podatności na ataki. W obszarze tym NIK zidentyfikowała także przypadki **wykorzystywania ochrony informacji poprzez nadawanie klauzul niejawności dokumentom sporządzonym i wykorzystywanym wcześniej jako jawne, w celu uniemożliwienia wglądu do nich na podstawie przepisów o dostępie do informacji publicznej**. Działania takie miały również bezpośredni wpływ na sposób prowadzenia badań przez kontrolerów NIK.

W ocenie NIK **zagadnienie upubliczniania wyników audytów bezpieczeństwa jest złożone**.

Z jednej strony mogą one zawierać szereg informacji, atrakcyjnych dla ewentualnego napastnika, np. dotyczących charakterystyki środków technicznych i organizacyjnych związanych z bezpieczeństwem informacji, tj. stwierdzone podatności, luki i słabości wraz z ich konsekwencjami oraz zalecenia co do sposobów ich wyeliminowania.

Z drugiej strony ograniczenie dostępu do informacji o stwierdzonych w trakcie audytów nieprawidłowościach:

[12] Zgodnie z ustaleniami kontroli we wszystkich jednostkach (poza KRUS) SZBI był w trakcie budowy a decyzje o rozpoczęciu jego budowy były podejmowane w okresie objętym kontrolą (2014–2015).

[13] Wyrok z dnia 9 kwietnia 2015 r. (sygn. akt K 14/13(ZU OTK nr 4A/2015, poz. 45).

- uniemożliwia zapoznanie się z oceną bezpieczeństwa systemów ich wszystkim użytkownikom (w przypadku realizacji przez te systemy zadań publicznych dotyczy to potencjalnie wszystkich obywateli);
- utrudnia i komplikuje wykorzystywanie wyników audytu w jednostce, np. ograniczając ich obieg, dostępność i znajomość;
- rodzi, w pewnym stopniu fałszywe, przekonanie o bezpieczeństwie oraz poczucie, że naprawienie stwierdzonych luk i podatności nie jest pilne, bo wiedza o nich nie jest szeroko dostępna, więc solidnie ukryta;
- może być nadużywane przez kierownictwo jednostki w związku z naturalnym dążeniem do przedstawiania swojej pracy i kierowanej przez siebie jednostki w jak najlepszym świetle, a tym samym zniechęcać do podejmowania działań naprawczych.

Wsparcie firm zewnętrznych

Połowa skontrolowanych jednostek korzystała przy realizacji procesów zapewnienia bezpieczeństwa informacji w istotnym zakresie ze wsparcia firm zewnętrznych. Dotyczyło to:

- pełnego przekazania eksploatacji i nadzorowania systemu zewnętrznemu operatorowi, który został zobowiązany w umowie do zapewnienia bezpieczeństwa systemu i przetwarzanych w nim danych (KRUS);
- powierzenia budowy systemu bezpieczeństwa informacji dla całej instytucji zewnętrznej firmie, która zobowiązana została do przeprowadzenia audytu bezpieczeństwa, prac analitycznych, ostatecznego wdrożenia SZBI i wsparcie jego dalszego funkcjonowania (SG);
- opracowania dokumentów i szablonów dokumentów związanych z bezpieczeństwem informacji, zapewnienia bezpieczeństwa systemu w trakcie jego rozbudowy, prowadzenia audytów obejmujących różne aspekty bezpieczeństwa (MS).

W ocenie NIK **wykorzystywanie wsparcia zewnętrznego obejmującego bezpieczeństwo informacji pozwala na zmniejszenie zaangażowania własnych zasobów, umożliwia zastosowanie nowoczesnych produktów dostępnych na rynku komercyjnym oraz ułatwia zintegrowanie funkcjonalności związanych z bezpieczeństwem systemów już w trakcie ich budowy. Takie działanie wiąże się jednak z występowaniem szeregu ryzyk**, które zadaniem NIK, można, przy odpowiednim zarządzaniu nimi, uznać za akceptowalne. Wymaga to od jednostki m.in. opracowania zasad szacowania takiego ryzyka na styku jednostka – firma zewnętrzna, zarządzania nim, a także wypracowania odpowiednich mechanizmów nadzoru i kontroli. Niestety w kontrolowanych jednostkach działania te nie zostały podjęte.

Źródło: Fotolia.com

2.3 Uwagi i wnioski

Wyniki tej kontroli, podobnie jak wyniki poprzedniej kontroli NIK pt. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* wskazują na **brak systemowych, kompleksowych rozwiązań dotyczących bezpieczeństwa IT**. W konsekwencji działania podejmowane w związku z koniecznością zapewniania bezpieczeństwa działania systemów informatycznych były w większości kontrolowanych jednostek chaotyczne, intuicyjne i fragmentaryczne. Obowiązujące przepisy prawne nie dostarczały konkretnych wytycznych odnośnie sposobów spełnienia poszczególnych wymagań gwarantujących odpowiedni poziom bezpieczeństwa teleinformatycznego, a kontrolowane podmioty nie zawsze widziały konieczność podejmowania innych działań związanych z bezpieczeństwem informacji, niż zapisane w ustawie o ochronie informacji niejawnych oraz ustawie o ochronie danych osobowych.

W ocenie NIK, **konieczne jest zatem opracowanie i wprowadzenie na szczeblu centralnym, obowiązujących wszystkie podmioty publiczne, generalnych zaleceń i wymagań dotyczących zapewnienia bezpieczeństwa IT**. Za wzór mogłyby posłużyć np. zalecenia opisane w Polskich Normach[14]. Zdaniem NIK zalecenia dla podmiotów publicznych powinny zostać opracowane przez ministra właściwego w sprawach cyfryzacji.

Ponadto NIK zwraca uwagę na problematykę związaną z ujawnianiem wyników audytów dotyczących bezpieczeństwa IT przeprowadzanych w kontrolowanych jednostkach. W ocenie NIK istnieje potrzeba systemowego rozwiązania tej kwestii, w sposób zapewniający dostęp obywateli do informacji o działalności podmiotów publicznych, z jednoczesnym zachowaniem ograniczeń w dostępie do wiedzy o stosowanych środkach i metodach zapewniających bezpieczeństwo przetwarzanych informacji.

Źródło: Fotolia.com.

14 PN-ISO/IEC 27001:2007.

3 WAŻNIEJSZE WYNIKI KONTROLI

3.1 Charakterystyka obszaru objętego kontrolą

3.1.1. Ogólne informacje dot. obszaru objętego kontrolą

W ciągu ostatnich kilkunastu lat w znaczącym stopniu wzrósł zakres wykorzystywania technik informatycznych. Coraz częściej mamy do czynienia z działalnością człowieka wspomaganą lub zastępowaną poprzez maszynowe przetwarzanie informacji. Rosnący stopień wykorzystania informatyki przez biznes, instytucje rządowe i administrację publiczną spowodował, oprócz oferowania nowej jakości towarów i usług, stopniowe uzależnianie ich dostępności od sprawnego funkcjonowania systemów informatycznych i łącznościowych. Od wielu z tych zmian nie ma już możliwości odwrotu. Nowe usługi i towary stały się powszechne i standardowe, a dotychczasowe metody ich świadczenia i dostarczania – przestarzałe oraz nieopłacalne.

Analizując funkcjonowanie instytucji państwowych można stwierdzić, że systemy komputerowe są praktycznie wszechobecne. Rozpoczynając od szeroko wykorzystywanych programów biurowych, za pomocą których powstają wszelkiego rodzaju dokumenty, poprzez systemy księgowości, kończąc na ogromnych, ogólnokrajowych aplikacjach obsługujących ubezpieczenia społeczne i zdrowotne, rejestry dokumentów oraz ewidencje prawne lub majątkowe.

Nowe narzędzia ułatwiając dostęp do informacji i szybkość ich przekazywania przyczyniły się również do powstania nowych zagrożeń. Dotychczasowe, wypracowane przez wieki doświadczenia, sposoby ochrony danych powierzanych administracji państwowej przestały być wystarczające. Prowadzonych obecnie, z wykorzystaniem nowoczesnej technologii, spraw nie można już zamknąć w metalowej szafie, umieścić w teczce, przesłać w zaklejonej kopercie, a często nawet przekazać do archiwum. Wymagane są: stosowanie zupełnie innych systemów zabezpieczeń oraz ochrona przed zupełnie nowymi zagrożeniami. Dynamiczna zmiana sposobów „załatwiania spraw" przez administrację spowodowała powstanie niebezpiecznej luki pomiędzy świadomością specjalistów stosujących nowoczesne rozwiązania, a świadomością kierownictwa określającego bezpieczne warunki funkcjonowania.

Sytuacja ta wymusza konieczność nowego spojrzenia na zasady przechowywania i przetwarzania informacji w tych systemach. Istotnym jest również właściwe usytuowanie procesu zapewnienia bezpieczeństwa w organizacji. Nie może być on jedynie domeną specjalistów IT – muszą brać w nim udział również użytkownicy, właściciele przetwarzanych informacji, a przede wszystkim kierownictwo jednostki.

3.1.2. Organizacja bezpieczeństwa informacji

Podstawowym aktem prawnym określającym wymogi dla państwowych systemów i rejestrów informatycznych jest ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (ustawa o informatyzacji). Ustawa ta określa m.in. zasady ustalania:

- ✓ minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi,
- ✓ Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji.

Zgodnie z art. 2 ust 1 ustawy o informatyzacji jej zapisy mają zastosowanie do podmiotów realizujących zadania publiczne określone przez ustawy m.in. do organów administracji rządowej, Kasy Rolniczego Ubezpieczenia Społecznego, Zakładu Ubezpieczeń Społecznych czy Narodowego Funduszu Zdrowia.

Art. 18 ww. ustawy zawiera delegację ustawową dla Rady Ministrów do określenia m.in. Krajowych Ram Interoperacyjności obejmujących zagadnienia interoperacyjności[15], czyli współdziałania i wymiany danych, różnych rozwiązań informatycznych oraz baz danych.

Realizując tę delegację **Rada Ministrów wydała rozporządzenie z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*** (rozporządzenie KRI).

W myśl § 15 ust. 1 ww. rozporządzenia, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (§ 20 ust. 1 rozporządzenia KRI). Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych w § 20 ust. 2 rozporządzenia KRI, w tym m.in.:

- zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (pkt 1);
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (pkt 2);
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy (pkt 3);
- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (pkt 4);
- bezzwłocznej zmiany uprawnień w przypadku zmiany zadań (pkt 5);
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji (pkt 6);
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (pkt 8);
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11);
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa (pkt 12 lit. h);

[15] Definicję ustawową tego określenia zawiera art. 3 pkt 18 ustawy o informatyzacji.

- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (pkt 14).

Zgodnie z § 20 ust. 3 rozporządzenia KRI, **wymagania, o których mowa w § 20 ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy** PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą w tym: PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W § 23 rozporządzenia KRI wskazano, że systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia KRI należy dostosować do wymagań określonych w rozdziale IV rozporządzenia KRI (minimalne wymagania dla systemów teleinformatycznych), nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie tego rozporządzenia.

Szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych zostały określone w rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*[16] wydanym na podstawie art. 10 ust. 4, art. 17 ust. 2 i art. 18 ust. 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[17].

Minister Spraw Wewnętrznych i Administracji wykonując delegację zawartą w art. 39 a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[18] wydał 29 kwietnia 2004 r. *rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*[19]. W § 6 tego rozporządzenia określono i zdefiniowano trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony i wysoki. Opis środków bezpieczeństwa stosowanych na poszczególnych poziomach określono w załączniku do ww. rozporządzenia.

Zapisy ustępów 1 i 2 § 20 rozporządzenia KRI nie dostarczają konkretnych wytycznych odnośnie sposobów spełnienia poszczególnych wymagań gwarantujących odpowiedni poziom bezpieczeństwa. W ustępie 3 tego rozporządzenia dopuszcza się całkowite odstąpienie od struktury wymagań określonej w ustępach 1 i 2 na rzecz stosowania Polskich Norm. Ustęp 4 wskazuje, że wymagania zapisane w ustępie 2 powinny zostać, w przypadkach uzasadnionych wynikami przeprowadzonej analizy ryzyka, uzupełnione o dodatkowe zabezpieczenia. Stosowanie § 20, jako całości, może być również – w przypadku konkretnych systemów – ograniczone, w związku z okresem ich eksploatacji oraz terminami istotnych modyfikacji.

16 Dz. U. Nr 128, poz. 1094.

17 Dz. U. z 2013 r. poz. 262, ze zm.

18 Dz. U. z 2015 r. poz. 2135, ze zm.

19 Dz. U. Nr 100, poz. 1024.

3.1.3. Obszar objęty kontrolą w świetle wyników dotychczasowych kontroli NIK

W Polsce jest eksploatowanych aktualnie kilkaset różnej wielkości systemów wykorzystywanych do realizacji zadań publicznych. Początki pracy niektórych z nich sięgają lat osiemdziesiątych ubiegłego wieku. Od ponad 20 lat polscy użytkownicy mają możliwość korzystania z sieci internet i pobierania z niej coraz większej ilości danych. Szacuje się, że w tym samym czasie powstały pierwsze niebezpieczne programy (wirusy komputerowe) wykonujące szkodliwe działania i przenoszące się pomiędzy komputerami bez wiedzy i świadomości ich właścicieli. Można więc stwierdzić, że w kraju mamy do czynienia z istotnym obszarem działalności administracji państwowej, narażonym od długiego już czasu na realne szkody. Obszar ten i dotyczące go zagrożenia podlegają dynamicznemu rozwojowi, tak jeśli chodzi o skalę (liczbę objętych nimi danych i realizowanych zadań), jak i zaawansowanie stosowanych narzędzi i rozwiązań technicznych (tak po stronie „przyjaznej" jak i „wrogiej").

Zgodnie ze sporządzonym przez GUS w 2013 roku wykazem „Systemy informacyjne administracji publicznej…"[20] **72 instytucje administracji państwowej eksploatowały 589 różnorodnych systemów informatycznych**[21].

Systemy te przetwarzają i wymieniają informacje w wirtualnym, krajowym obszarze zdefiniowanym, jako cyberprzestrzeń RP.

NIK, w wyniku zakończonej w 2015 r. kontroli, oceniła negatywnie działalność podmiotów państwowych w zakresie ochrony cyberprzestrzeni RP.

Administracja państwowa nie podjęła dotychczas niezbędnych działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski. Pomimo tego, że coraz większa część usług publicznych oraz istotnych aspektów życia społecznego i gospodarczego realizowanych jest obecnie w sieci Internet lub z wykorzystaniem systemów teleinformatycznych, bezpieczeństwo Polski w dalszym ciągu jest postrzegane jedynie w sposób konwencjonalny. Nie dostrzeżono, że powstała nowa kategoria zagrożeń, wymagająca pilnej reakcji państwa. **Kierownictwo najważniejszych instytucji publicznych nie posiada świadomości zagrożeń związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z nich nowych zadań administracji państwowej.**

Nie zostały dotychczas podjęte spójne i systemowe działania podmiotów państwowych, mające na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów. Przede wszystkim nie oszacowano ryzyka dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne. Nie określono struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań. Nie przygotowano procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią.

---

20 http://bip.stat.gov.pl/gfx/bip/userfiles/_public/bip/psp/bip_systemy_informacyjne_administracji_publicznej_2013.doc

21 Wykaz ten został opracowany dla celów statystyki publicznej i w związku z tym nie jest wykazem kompletnym. Brak jest obecnie systemowych rozwiązań dotyczących pozyskiwania informacji o funkcjonujących w kraju systemach teleinformatycznych przeznaczonych do realizacji zadań publicznych. Wynika to z usunięcia w 2010 r. z ustawy o informatyzacji art. 19, obligującego ministra właściwego ds. informatyzacji do prowadzenia Krajowej Ewidencji Systemów Teleinformatycznych i Rejestrów Publicznych.

W rezultacie, **działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej**. Skupiały się one do doraźnym, ograniczonym reagowaniu na bieżące wydarzenia oraz do biernym oczekiwaniu na rozwiązania, które w tym obszarze zaproponuje Unia Europejska. Kluczowym czynnikiem paraliżującym aktywność państwa w tym zakresie, był również brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych.

Wynikający z powyższych ustaleń **brak centralnych – krajowych wymagań i zaleceń dotyczących stworzenia bezpiecznego środowiska dla funkcjonujących systemów informatycznych powoduje powstawanie indywidualnych, lokalnych rozwiązań z zakresu bezpieczeństwa**.

Dotychczas nie podjęto systemowych działań na poziomie krajowym na rzecz ujednolicenia i zoptymalizowania na poziomie krajowym metod przeciwdziałania zagrożeniom występującym w cyberprzestrzeni, co powoduje powstawanie indywidualnych, często fragmentarycznych rozwiązań z zakresu bezpieczeństwa w poszczególnych podmiotach.

3.1.4. Metodyka badań kontrolnych dot. bezpieczeństwa systemów informatycznych

Złożona tematyka oraz brak szczegółowych regulacji prawnych, utrudnia wyznaczenie mierników i wyznaczników do przeprowadzenia kontroli w zakresie bezpieczeństwa konkretnych systemów informatycznych.

Kontrolę tego obszaru można jednak oprzeć o **opis procesu „DS5 Zapewnienie bezpieczeństwa systemów" występującego w uznanej, międzynarodowej metodyce COBIT 4.1.** Pozwala to, dzięki użyciu kompletnego zestawu celów kontrolnych dotyczących zapewnienia bezpieczeństwa, na dokonanie przekrojowej oceny warunków zapewnienia bezpieczeństwa przy jednoczesnym ograniczeniu jego szczegółowości. Zastosowanie metodyki umożliwia jednocześnie dokonanie obiektywnej oceny kontrolowanej działalności. Dzięki zdefiniowanym w niej miernikom oraz modelowi dojrzałości wyniki przeprowadzonych badań mogą być bezpośrednio wykorzystane do sporządzenia oceny kontrolowanej działalności.

Stosowanie metodyki COBIT w zakresie kontroli zagadnień informatycznych jest **zalecane w „Wytycznych w sprawie kontroli wewnętrznej w sektorze publicznym INTOSAI GOV 9100" oraz w „Podręczniku kontroli systemów informatycznych dla najwyższych organów kontroli opracowanym przez inicjatywę INTOSAI ds. Rozwoju (IDI)"**.

Zgodnie z tą metodyką wyróżnia się 6 stopni modelu dojrzałości:

0 Nieistniejące – całkowity brak rozpoznawalnych procesów. Przedsiębiorstwo nie dostrzegło nawet istnienia problemu, który wymaga rozwiązania.

1 Wstępne/doraźne – Istnieją dowody na to, że przedsiębiorstwo dostrzegło problemy wraz z koniecznością ich rozwiązania. Nie są to jednak ustandaryzowane procesy. Zamiast nich, do rozwiązywania poszczególnych problemów stosuje się doraźne podejście. Ogólne podejście do zarządzania nie jest podejściem zorganizowanym.

2 Powtarzalne lecz intuicyjne – procesy zostały rozwinięte do poziomu, na którym różne osoby wykonujące to samo zadanie postępują zgodnie z podobnymi procedurami. Nie ma formalnych szkoleń, standardowe procedury nie zostały zakomunikowane, a podjęcie odpowiedzialności pozostawiono jednostkom. Występuje wysoki poziom zależności od wiedzy poszczególnych osób, dlatego prawdopodobne jest występowanie błędów.

3 Zdefiniowane procesy – istnieją ustandaryzowane i udokumentowane procedury, które zostały zakomunikowane poprzez szkolenie. Pracownicy są upoważnieni do ich stosowania. Jest jednak mało prawdopodobne, że odstępstwa od stosowania procedur zostaną wykryte. Procedury nie są zaawansowane, a są raczej formalizacją istniejących praktyk.

4 Kontrolowane i mierzalne – kierownictwo monitoruje i ocenia zgodność z procedurami, a także podejmuje odpowiednie czynności, gdy procesy nie działają efektywnie. Procesy są stale doskonalone i stanowią źródło dobrych praktyk. W ograniczony lub fragmentaryczny sposób wykorzystywane są rozwiązania zautomatyzowane oraz narzędzia.

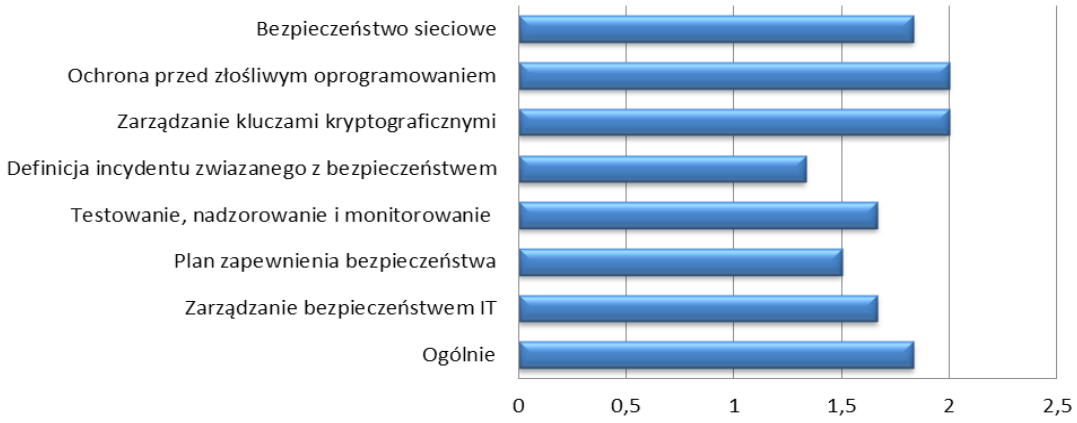
5 Zoptymalizowane – procesy zostały dopracowane do poziomu dobrej praktyki w oparciu o efekty ciągłego doskonalenia i modelowanie dojrzałości w innych przedsiębiorstwach. Technologia informatyczna jest wykorzystywana w zintegrowany sposób do automatyzacji toku pracy, zapewniając narzędzia służące poprawie jakości i wydajności oraz sprawiając, że przedsiębiorstwo szybko adaptuje się do zmieniających się warunków.

3.2 Wyniki kontroli w ujęciu przedmiotowym

3.2.1. Średni stopień dojrzałości badanych procesów w jednostkach objętych kontrolą[22]

Poniższe wykresy przedstawiają średnie oceny kontrolowanych jednostek dla poszczególnych obszarów objętych kontrolą sformułowane przez NIK przy zastosowaniu metodyki COBIT.

Wykres nr 1
Wspieranie bezpieczeństwa IT na poziomie całej jednostki

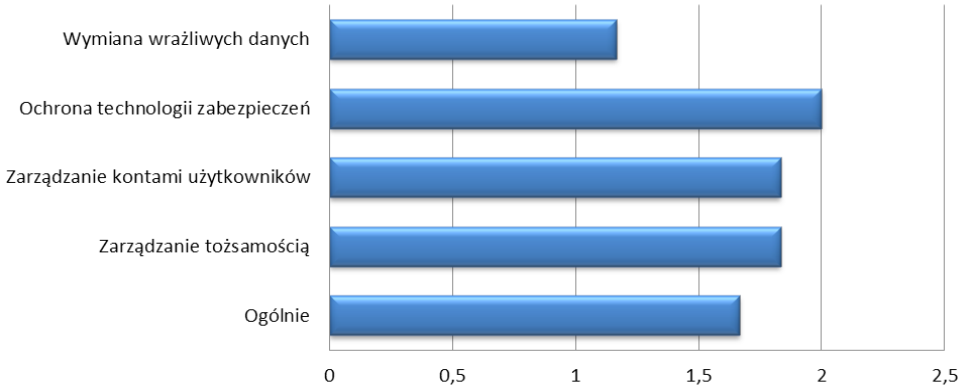


Źródło: Opracowanie własne NIK.

W zakresie wspierania bezpieczeństwa IT na poziomie całej jednostki najwyższe oceny wystąpiły w obszarze ochrony przed złośliwym oprogramowaniem i zarządzania kluczami kryptograficznymi, natomiast najniższe w zakresie definiowania incydentu związanego z bezpieczeństwem.

22 Przyjęta skala punktacji została przedstawiona w rozdziale 3.1.4.

Wykres nr 2
Wspieranie bezpieczeństwa IT na poziomie wybranego systemu



Źródło: Opracowanie własne NIK.

Najwyższe oceny w zakiesie wspierania bezpieczeństwa IT na poziomie wybranego systemu uzyskały kontrolowane jednostki w obszarze ochrony technologii zabezpieczeń, a najniższe w obszarze wymiany wrażliwych danych.

3.2.2. Zarządzanie bezpieczeństwem IT

Kierownictwo poszczególnych kontrolowanych jednostek posiadało świadomość potrzeby zapewnienia bezpieczeństwa informacji. Przy czym w przypadku niektórych (5) jednostek proces uzyskiwania wiedzy co do istnienia zagrożeń i konieczności przeciwdziałania im rozpoczął się stosunkowo niedawno. Podejście kierownictwa części jednostek do zagadnień bezpieczeństwa podlegało dynamicznym zmianom, które zachodząc również w trakcie działań kontrolnych, wpływały na dokonane ustalenia.

Stworzone w kontrolowanych jednostkach systemy zapewnienia bezpieczeństwa posiadały różne architektury, nie były to jednak rozwiązania optymalne z powodu:

- ✓ braku koordynacji pomiędzy komórkami organizacyjnymi realizującymi różne zadania z zakresu zapewnienia bezpieczeństwa;
- ✓ niespójnego określenia kompetencji poszczególnych jednostek, co prowadziło do nakładania się odpowiedzialności lub pozostawiania niektórych zagadnień praktycznie bez nadzoru;
- ✓ ograniczenia odpowiedzialności za bezpieczeństwo informacji do komórki odpowiedzialnej za wdrażanie i administrowanie systemami teleinformatycznymi;
- ✓ przekazywania znacznego zakresu zadań związanych z zapewnieniem bezpieczeństwa informacji podmiotom zewnętrznym bez zidentyfikowania i zredukowania wynikających z tego ryzyk oraz zorganizowania odpowiedniego systemu nadzoru i kontroli realizacji tych zadań;
- ✓ niedostosowania wielkości zasobów ludzkich, finansowych i organizacyjnych do liczby i złożoności zadań związanych z bezpieczeństwem informacji;
- ✓ tworzenia samodzielnych, jednoosobowych stanowisk odpowiedzialnych za istotne elementy systemu zapewnienia bezpieczeństwa bez właściwej analizy pracochłonności lub określenia zastępstw na czas absencji i urlopów;
- ✓ niewykorzystywania doświadczeń wynikających ze zrealizowanych wcześniej przedsięwzięć dotyczących bezpieczeństwa informacji.

Cele strategiczne w zakresie bezpieczeństwa informacji formułowane były wadliwie, z pominięciem niektórych niezbędnych składników tych celów m.in. nie określano mierników służących do monitorowania realizacji tych celów, horyzontu czasowego w którym te cele zostaną zrealizowane, a także nie określano zasobów niezbędnych do ich realizacji.

Kontrolowane jednostki nie dokonały identyfikacji i ewidencji swoich kluczowych zadań wraz z zasobami niezbędnymi do ich realizacji.

Identyfikacja informacji wrażliwych (tj. zasobów krytycznych dla instytucji) ograniczona była do informacji chronionych ustawowo (wynikających z uodo i uoin). Nie identyfikowano informacji, których ochrona nie jest prawnie wymagana, a które mogą być wykorzystane przeciwko instytucji poprzez ich ujawnienie, zablokowanie lub zmanipulowanie.

Żadna z kontrolowanych jednostek nie nie dokonywała wstępnego szacowania kosztów (w tym również niematerialnych) ewentualnego naruszenia bezpieczeństwa (poufności, integralności i dostępności) informacji, co wynikało przede wszystkim z niepełnej identyfikacji i ewidencji informacji wrażliwych.

Okresowe informowanie kierownictwa o stanie bezpieczeństwa informacji oraz o związanych z nim ważnych wydarzeniach było realizowane tylko w niektórych jednostkach. Ponadto ich przekazywanie nie było związane z cykliczną realizacją odpowiedniego procesu, tylko wynikało głównie z przyczyn występujących doraźnie, np. incydentu bezpieczeństwa.

W kontrolowanych jednostkach istniały znane i dostępne dla wszystkich pracowników źródła informacji o zagadnieniach związanych z bezpieczeństwem teleinformatycznym – była to przede wszystkim korespondencja kierowana do pracowników za pomocą poczty elektronicznej oraz dane zamieszczane w portalach intranetowych. Przeprowadzona podczas kontroli analiza tych informacji wskazała, że dotyczyły one wewnętrznych przepisów (prezentowany stan prawny nie zawsze był aktualny) i instrukcji oraz zaleceń dla pracowników dotyczących zagrożeń, które wydarzyły się wcześniej w danej instytucji.

Proces szacowania ryzyka w jednostkach kontrolowanych był realizowany w ograniczonej skali, co wynikało m.in. z:

- ✓ nieokreślenia standardowej metodyki szacowania ryzyka dla jednostek realizujących zadania publiczne;
- ✓ braku właściwego przeszkolenia pracowników zobowiązanych do prowadzenia szacowania ryzyka, szczególnie w przypadkach prowadzenia tego procesu przy pomocy narzędzi informatycznych;
- ✓ błędnego utożsamiania specyficznego procesu szacowania ryzyka wynikającego z treści Programu Ochrony Cyberprzestrzeni RP (dotyczącego jedynie ryzyk dotyczących funkcjonowania cyberprzestrzeni) z procesem związanym z bezpieczeństwem informacji, którego zakres jest znacznie szerszy;
- ✓ nieprzygotowania danych niezbędnych do przeprowadzenia szacowania ryzyka i jednolitej dla całej instytucji metodyki pozwalającej porównywać poszczególne ryzyka, wykazu aktywów wraz z właścicielami i oszacowaniem ich wartości oraz kryteriów akceptacji ryzyka.

3.2.3. Plan zapewnienia bezpieczeństwa

W żadnej ze skontrolowanych jednostek nie opracowano rzetelnego planu zapewnienia bezpieczeństwa.

Część jednostek nie opracowała w ogóle dokumentu pełniącego rolę planu zapewnienia bezpieczeństwa, natomiast część opracowała taki dokument, jednakże został on we wszystkich przypadkach oceniony przez NIK jako nierzetelny.

Główne nieprawidłowości polegały na tym, że plan ten był:

- **nieaktualny lub niekompletny** – kierownictwo instytucji miało świadomość tych wad i prowadzono prace mające na celu opracowanie docelowego planu. Pomimo formułowania odpowiednich wymagań plany nie były cyklicznie przeglądane i aktualizowane, co powoduje stopniową utratę aktualności związaną z postępem technicznym, zmianami organizacyjnymi i zmianami w obowiązującym prawie;
- **rozproszony** – plan składał się z wielu niespójnych, wytworzonych niezależnie dokumentów, instrukcji i procedur stosowanych doraźnie i lokalnie. Brakowało powiązania tych dokumentów oraz określenia hierarchii ich ważności;
- **ograniczony** – dotyczył jedynie szczególnych rodzajów danych – danych osobowych lub informacji niejawnych i opracowane były zgodnie ze szczegółowymi wymaganiami ustawowymi. Po dokonaniu, w niektórych jednostkach nawet niewielkich modyfikacji rozszerzających ich zakres przedmiotowy na inne przetwarzane informacje, plany takie faktycznie nie zapewniały właściwego poziomu bezpieczeństwa IT;
- **niezatwierdzony** (w pewnym zakresie) – nie obejmował elementów szczegółowych, opracowanych jako odrębne polityki lub procedury. Niezatwierdzone wersje takich szczegółowych dokumentów były jednak faktycznie wykorzystywane, w ramach stosowania tzw. dobrych praktyk;
- **nieadekwatny** – niektóre z planów zostały opracowane na zlecenie kontrolowanych jednostek przez podmioty zewnętrzne, skutkiem czego było umieszczenie w tych dokumentach zapisów niezwiązanych ze specyfiką danej instytucji, a pochodzących z różnego rodzaju szablonów wykorzystywanych przez autorów do opracowania planu. Część specyficznych dla danej jednostki zagadnień dotyczących bezpieczeństwa IT, nie była takimi planami objęta.

3.2.4. Testowanie, nadzorowanie i monitorowanie bezpieczeństwa

Wszystkie kontrolowane jednostki wykorzystywały do budowy systemów zapewnienia bezpieczeństwa informacji wyniki audytów: wynikających z realizacji obowiązku określonego rozporządzeniem KRI lub wymaganych dla utrzymania certyfikatów dotyczących bezpieczeństwa informacji, a także zleconych bądź wynikających z planowej działalności kontrolnej.

Rozporządzenie KRI wymaga zapewnienia od maja 2012 r. okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, powtarzanego nie rzadziej niż raz na rok. W ocenie NIK przekazane kierownictwom instytucji informacje wynikające z audytów przeprowadzonych zgodnie z ww. wymaganiami stanowiły istotny impuls do rozpoczęcia lub zintensyfikowania prac nad stworzeniem systemów zapewnienia bezpieczeństwa informacji.

W żadnej ze skontrolowanych jednostek nie stwierdzono prawidłowo funkcjonującego systemu reagowania na incydenty związane z bezpieczeństwem informacji. Stwierdzone nieprawidłowości dotyczyły w szczególności:

1) braku definicji incydentu pozwalającej użytkownikom jednoznacznie zidentyfikować i wstępnie ocenić zdarzenie, z którym się zetknęli; dotyczyło to również braku określenia kryteriów poziomu istotności dla incydentu;
2) braku realnie funkcjonujących procedur dotyczących sposobów zgłaszania incydentów, ich rejestrowania oraz sposobu reagowania;
3) nieskutecznej struktury rejestru incydentów, prowadzonego niezależnie w różnych miejscach instytucji lub połączonego z rejestrami dotyczącymi wsparcia, awarii i błędów technicznych;
4) braku właściwej współpracy z wykonawcami zewnętrznymi, co powodowało:
   a) nierejestrowanie incydentów stwierdzanych przez wykonawców zewnętrznych podczas wykorzystywania infrastruktury instytucji, gdyż nie byli oni zobowiązywani w umowach do zgłaszania takich incydentów do rejestru;
   b) brak wymiany informacji o incydentach pomiędzy rejestrami prowadzonymi przez usługodawców zewnętrznych, a korzystającą z ich usług instytucją. Sytuacja taka miała również miejsce w przypadku, gdy w ramach outsourcingu istotne zadania instytucji związane z bezpieczeństwem realizowane były przez firmę zewnętrzną.

Zdaniem NIK to właśnie powyższe braki w systemie zbierania i analizy incydentów w głównej mierze powodują niski poziom wiedzy w poszczególnych jednostkach objętych kontrolą, co do rodzaju i charakteru zagrożeń jakim podlegają.

3.2.5. Zarządzanie kluczami kryptograficznymi[23]

Żadna z kontrolowanych jednostek nie posiadała polityki zabezpieczeń kryptograficznych. Nie prowadzono analiz dotyczących możliwości i zakresu wykorzystania technik kryptograficznych do zabezpieczenia istotnych informacji. W przypadkach, w których korzystano z certyfikatów cyfrowych do identyfikacji użytkowników w systemach informatycznych, dostawcy tych rozwiązań opracowywali również niezbędne procedury, instrukcje i polityki, wdrażane następnie w kontrolowanych jednostkach.

W systemach, w których dopuszczano do zdalnego dostępu dla celów administracyjnych i serwisowych, informacje były zabezpieczane za pomocą rozwiązań kryptograficznych.

3.2.6. Ochrona przed złośliwym oprogramowaniem

We wszystkich kontrolowanych jednostkach stosowano zabezpieczenia przed szkodliwym oprogramowaniem. Wykorzystywane w tym celu narzędzia pochodziły od różnych dostawców, posiadały różną funkcjonalność oraz były z różnym zaangażowaniem konserwowane i obsługiwane przez pracowników poszczególnych jednostek.

Systemy te generowały raporty i dzienniki, które jednak nie we wszystkich przypadkach były systematycznie przeglądane i analizowane. W kontrolowanych jednostkach nie opracowano formalnych zasad przeglądania i analizowania raportów i dzienników dotyczących efektów działania zabezpieczeń przed szkodliwym oprogramowaniem. Z udzielonych wyjaśnień wynikało, że takie

[23] Jednym z najlepszych sposobów zabezpieczenia informacji jest wykorzystanie technik kryptograficznych, które pozwalają chronić poufności i autentyczność informacji w szczególności podczas jej przesyłania np. za pomocą ogólnie dostępnych sieci. Szyfrowanie i deszyfrowanie informacji odbywa się za pomocą kluczy kryptograficznych.

przeglądy i analizy leżą w obowiązkach poszczególnych administratorów systemów i sieci, jednak w żadnym z kontrolowanych przypadków nie przedstawiono dokumentów potwierdzających ich przeprowadzanie, opisujących wyniki i zastosowane w ich konsekwencji działania.

3.2.7. Bezpieczeństwo sieciowe

W kontrolowanych jednostkach w zakresie zapewnienia bezpieczeństwa sieciowego stwierdzono brak skutecznych mechanizmów kontrolnych:

- ✓ **nad nieużywanymi lub niepodłączonymi portami przełączników urządzeń dostępowych,**
- ✓ **przed nieautoryzowanym podłączeniem obcych urządzeń do sieci jednostki,**
- ✓ **w zakresie przepływu ruchu sieciowego wewnątrz sieci jednostki.**

Przetwarzanie mobilne posiadało wyraźnie niższy poziom bezpieczeństwa, wynikający z pomocniczej roli jaką spełnia, co skutkowało tym, że we wszystkich skontrolowanych jednostkach (poza częścią systemów SG) podstawowe systemy wykorzystywały jedynie połączenia przewodowe.

Wystąpiły przypadki zobowiązania użytkowników urządzeń mobilnych do samodzielnego administrowania ich oprogramowaniem antywirusowym, co zdaniem NIK powodowało powstanie poważnego ryzyka, że użytkownicy będą wykonywali te obowiązki nierzetelnie.

W jednej z kontrolowanych jednostek stwierdzono, że nieprawidłowe eksploatowanie oprogramowania zabezpieczającego przed złośliwym oprogramowaniem spowodowało liczne przypadki zawirusowania stacji roboczych, docierania do pracowników e-maili z niebezpiecznymi odnośnikami, jak również funkcjonowanie zainstalowanej bez wiedzy użytkowników sieci typu „botnet" obejmujący 24 komputery biurowe. Przyczynami tych nieprawidłowości były źle realizowane obowiązki administratora oraz brak lub nieaktualne oprogramowanie antywirusowe.

Bezpieczeństwo jednego z systemów objętych kontrolą oparte zostało na założeniu, że wszystkie jego elementy są odseparowane od sieci publicznej. Instytucja administrująca tym systemem nie posiadła jednak możliwości technicznych i prawnych aby weryfikować ciągłość i jakość tej separacji. W toku kontroli stwierdzono udokumentowany przypadek utraty tej separacji, jednakże nie spowodowało to zmiany przez administratora zasad i podstaw zapewnienia bezpieczeństwa.

3.2.8. Zarządzanie tożsamością i kontami użytkowników

We wszystkich kontrolowanych jednostkach funkcjonowały formalne procedury związane z nadawaniem uprawnień do dostępu do systemów objętych kontrolą. Przeprowadzona analiza wskazała, że wprowadzone procedury nie zabezpieczały dostatecznie przed wystąpieniem nieprawidłowości.

NIK stwierdziła bowiem że:

- ✓ nie uwzględniono w stosowanej procedurze opinii właściciela informacji (np. dyrektora departamentu merytorycznego), do których udzielany był dostęp. Główną przyczyną tego stanu rzeczy były, w ocenie NIK błędy w procesie identyfikacji zasobów i nieprzypisanie danych zasobów do właściciela;
- ✓ nie przeprowadzano okresowych kontroli aktualności kont użytkowników i zasadności udzielonych uprawnień, w tym szczególnie dla kont tzw. uprzywilejowanych;
- ✓ brak było specyficznych procedur dotyczących udzielania uprawnień uprzywilejowanych, w tym modyfikowania własnych uprawnień przez administratorów;

- ✓ wystąpiła niezgodność stopnia komplikacji haseł dostępu do kont i dozwolonej liczby kolejnych błędnych logowań z wymaganiami formalnymi określonymi przez jednostkę;
- ✓ brak było wymogu zmiany hasła otrzymanego od administratora po pierwszym zalogowaniu;
- ✓ nie zapewniono właściwego obiegu informacji w przypadku długich nieobecności i zwolnień pracowników, co skutkowało pozostawianiem aktywnych kont użytkowników długotrwale nieobecnych;
- ✓ tworzono konta grupowe, bez właściwego uzasadnienia, udokumentowania i zatwierdzenia;
- ✓ posługiwano się niezabezpieczoną drogą mailową do przesyłania informacji odnośnie przyjęć, zwolnień i absencji pomiędzy działem kadr, a działem IT.

3.2.9. Ochrona technologii zabezpieczeń

W żadnej ze skontrolowanych jednostek nie wprowadzono formalnie procedury zamiany domyślnych lub tymczasowych haseł w użytkowanym i instalowanym sprzęcie podłączanym do sieci. W niektórych jednostkach pracownicy obsługujący i instalujący taki sprzęt z własnej inicjatywy zmieniali domyślne hasła, opierając się na swoim doświadczeniu i dobrych praktykach.

W większości kontrolowanych jednostek nie była prowadzona ewidencja aktywów wspierających, związanych z zapewnieniem bezpieczeństwa informacji, w związku z czym, nie przyporządkowano im istotności, poziomów ochrony i właścicieli.

Wystąpiły przypadki pozostawienia administratorom systemów informatycznych możliwości samodzielnego modyfikowania własnych uprawnień.

W czasie kontroli dokonano przeglądu losowej próby umów z dostawcami usług i wykonawcami produktów związanych z obiegiem informacji i funkcjonowaniem systemów informatycznych. We wszystkich przypadkach stwierdzono, że zawierały one klauzule dotyczące zachowania poufności informacji uzyskanych w trakcie realizacji umowy przez podmiot zewnętrzny.

3.2.10. Wymiana wrażliwych danych

Problematyka warunków wymiany, transmisji i sporządzania kopii informacji wrażliwych jest ściśle powiązana z poziomem wiedzy użytkowników w zakresie klasyfikowania danych i określania ich wartości.

W kontrolowanych jednostkach poza zakresami danych wrażliwych wynikających wprost z uodo i uoin, praktycznie nie identyfikowano innych danych mających szczególne znaczenie dla instytucji i realizowanych przez nie zadań. Ten brak przekładał się bezpośrednio na zakres zapewnienia bezpieczeństwa w zakresie ich wymiany, transmisji i sporządzania kopii.

Nie określano formalnie zasad zabezpieczania kryptograficznego kopii bezpieczeństwa systemów.

Nie przestrzegano zasady przesyłania jednej z kopii bezpieczeństwa w miejsce niezagrożone skutkami ewentualnej katastrofy (w siedzibie instytucji lub ośrodku przetwarzania danych).

3.3 Wyniki kontroli w ujęciu podmiotowym

3.3.1. Zestawienie poszczególnych ocen kontrolowanych jednostek

Poniższa tabela przedstawia oceny kontrolowanych jednostek dla poszczególnych obszarów objętych kontrolą sformułowane przez NIK przy zastosowaniu metodyki COBIT.

Tabela nr 2

		KRUS	MS	MSP	NFZ	SG	MSW
Ocena ogólna		**3**	**2**	**2**	**2**	**1**	**1**
Wspieranie bezpieczeństwa IT na poziomie całej jednostki	Ogólnie	3	2	2	2	1	1
	Zarządzanie bezpieczeństwem IT	3	1	3	1	1	1
	Plan zapewnienia bezpieczeństwa	3	2	1	1	1	1
	Testowanie, nadzorowanie i monitorowanie bezpieczeństwa	2	2	2	3	1	0
	Definicja incydentu związanego z bezpieczeństwem	2	1	1	1	1	1
	Zarządzanie Kluczami Kryptograficznymi	1	3	3	3	1	1
	Ochrona przed złośliwym oprogramowaniem	3	2	2	2	1	2
	Bezpieczeństwo sieciowe	3	2	2	2	1	1
Wspieranie bezpieczeństwa IT na poziomie wybranego systemu	Ogólnie	2	2	2	2	2	1
	Zarządzanie tożsamością	2	2	1	2	2	2
	Zarządzanie kontami użytkowników	2	2	2	2	2	1
	Ochrona technologii zabezpieczeń	3	3	2	2	2	0
	Wymiana wrażliwych danych	2	2	1	1	1	0

0 – niezdefiniowany, 1 – początkowy/doraźny, 2 – powtarzalny lecz intuicyjny, 3 – zdefiniowany, 4 – kontrolowany i mierzalny, 5 – zoptymalizowany.

Źródło: Opracowanie własne NIK.

Najwyższą ocenę, jaką uzyskała kontrolowana jednostka w badanych obszarach była ocena na poziomie 3. Otrzymało ją KRUS. Najniższą ocenę uzyskało MSW i SG – 1. Ministerstwa Sprawiedliwości i Skarbu Państwa oraz NFZ uplasowały się na tym samym poziomie – 2.
KRUS otrzymała ocenę na poziomie 3 w 6 obszarach. MSW otrzymało ocenę na poziomie 0 w 4 obszarach.

3.3.2. Kasa Rolniczego Ubezpieczenia Społecznego

W oparciu o stosowany w metodyce COBIT 4.1 Model dojrzałości, **NIK oceniła poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w KRUS jako *zdefiniowany***.
KRUS była jedyną jednostką objętą badaniem która posiadała Certyfikat potwierdzający, iż obsługa ubezpieczonych i świadczeniobiorców w zakresie zadań wynikających z ustawy o ubezpieczeniu

społecznym rolników[24] spełnia wymagania normy PN-ISO/IEC 27001:2007[25] (Norma). Objęty szczegółową kontrolą system FARMER był zarządzany w modelu pełnego outsourcingu, co oznacza, że zarówno usługi jak i infrastruktura została powierzona w całości wykonawcy zewnętrznemu[26].

W jednostce tej wprowadzono system bezpieczeństwa informacji w ramach Zintegrowanego Systemu Zarządzania, co zdaniem NIK świadczy o tym, że kierownictwo było świadome potrzeby zapewnienia bezpieczeństwa. W ocenie Izby wdrożony system wymaga jednak poprawy i udoskonalenia. W KRUS zdefiniowano główne procedury bezpieczeństwa i w ocenie NIK były one wzajemnie kompatybilne, niemniej jednak Izba wniosła szereg uwag do czytelności i kompletności tych procedur. Stwierdzono braki w zakresie podmiotowym (nie do wszystkich systemów opracowano procedury), jak również w zakresie przedmiotowym (nie wszystkie zagadnienia zostały uregulowane, np. brak było procedur dotyczących zawieszania uprawnień dostępu do systemów).

Przyjęta koncepcja powierzenia zasobów KRUS wykonawcy zewnętrznemu m.in. w zakresie systemów służących realizacji podstawowych ustawowych zadań nie została poprzedzona stosowymi analizami, np. nie określono sposobu szacowania ryzyka związanego z utratą informacji w sytuacji powierzenia zasobów firmie zewnętrznej. Co za tym idzie, w ocenie NIK, nie zapewniono odpowiednich zasobów (przede wszystkim kadrowych[27]) oraz nie wypracowano realnych narzędzi nadzoru nad bezpieczeństwem informacji. Przykładowo w umowach z wykonawcą nie przewidziano przeprowadzania testów bezpieczeństwa. Dlatego też, zdaniem NIK, istniało wysokie ryzyko, że usługi świadczone przez podmioty zewnętrzne mogły nie spełniać opracowanych w kontrolowanej jednostce wymagań dotyczących bezpieczeństwa.

W stworzonym w KRUS systemie zarządzania bezpieczeństwem informacji określono zasady oceny procedur i ich aktualizacji, a proces zapewnienia bezpieczeństwa był monitorowany przez okresowe audyty. Jednakże określonym celom w zakresie bezpieczeństwa nie przypisano miernika, oraz zasobów niezbędnych do ich osiągnięcia.

Stworzono system zbierania i analizy incydentów, jednakże był on niekompletny, tj. nie obejmował m.in. incydentów obsługiwanych przez administratorów oraz incydentów systemu FARMER. Nierzetelna sprawozdawczość wynikająca z niekompletnego systemu rejestrowania incydentów jak i również stwierdzona wadliwość miernika procesu zarządzania bezpieczeństwem, w ocenie NIK, skutkowało pozbawieniem kierownictwa KRUS podstawowego narzędzia monitorowania poziomu bezpieczeństwa informacji.

W KRUS opracowano Klasyfikację Informacji w ramach procedur Zintegrowanego Systemu Zarządzania, jednakże NIK stwierdziła, że nie wszystkim informacjom nadano właściwy poziom zabezpieczeń, w szczególności dotyczyło to kodów źródłowych. Nie mniej jednak, niezależnie od uregulowań wewnętrznych, zasoby te w praktyce były właściwie chronione.

W obszarze zarządzania kontami użytkowników systemu informatycznego objętego kontrolą stwierdzono nieprawidłowości, które w ocenie Izby obniżają jego bezpieczeństwo. Nieprawidłowości polegały m.in. na nieprzeprowadzaniu okresowych przeglądów aktualności

24 Ustawa z dnia 20 grudnia 1990 r. (Dz. U. z 2016 r. poz. 277).

25 W okresie objętym kontrola funkcjonowały dwa takie certyfikaty Nr. I-19/1/2014 wydany 21 listopada 2014 r. oraz Nr JKI -2/2/2011 z dnia 22 listopada 2011 r.

26 Był on utrzymywany i administrowany w ośrodkach obliczeniowych wykonawcy (firmy Zeto i Unizeto), natomiast pracownicy KRUS mieli do niego dostęp poprzez sieć WAN.

27 Według ustaleń kontroli minimalny zespół zajmujący się nadzorem nad realizacją umowy przez wykonawcę powinien liczyć 3 osoby, gdy tymczasem czynności wykonywał jeden pracownik, któremu powierzono również inne zadania.

i adekwatności uprawnień również w systemie FARMER, niezawieszaniu uprawnień pomimo długotrwałej nieobecności, co wynikało, zadaniem NIK, z braku procedur w tym zakresie, niezgodności maski hasła do sytemu FARMER z przyjętymi procedurami wewnętrznymi.

Przy czym NIK zauważyła, że w KRUS podejmowane były działania zmierzające do systemowego usunięcia tych nieprawidłowości.

3.3.3. Ministerstwo Sprawiedliwości

W oparciu o stosowany w metodologii COBIT 4.1 model dojrzałości **NIK oceniła w Ministerstwie Sprawiedliwości poziom zarządzania procesem zapewniania bezpieczeństwa IT oraz wspierania bezpieczeństwa w odniesieniu do systemu teleinformatycznego ksiąg wieczystych jako *powtarzalny* lecz *intuicyjny***.

Funkcjonująca dokumentacja polityki bezpieczeństwa była niedostosowana do specyfiki Ministerstwa i niespójna (niejednolita terminologia, różne opisy tych samych terminów, zamienne stosowanie zupełnie odmiennych pojęć, niejasne i wzajemnie dublujące się uprawnienia i obowiązki). Brakowało również jasnego określenia poziomów koniecznego bezpieczeństwa dla poszczególnych dokumentów składających się na tę politykę i ich przeznaczenia. Dokumentacja ta została wytworzona przez podmiot zewnętrzny i od zatwierdzenia w 2012 r. nie była aktualizowana.

Stwierdzono również braki dokumentacji potwierdzającej zapoznawanie się pracowników z polityką oraz chaos organizacyjny dot. przechowywania stosownych oświadczeń w 2014 r. Powyższe, zdaniem Izby, wskazywało na niespełnienie wymogów § 20 ust. 2 pkt 4 rozporządzenia KRI w zakresie *zapewnienia warunków umożliwiających realizację i egzekwowanie podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w nim w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji*.

Brak realnego wdrożenia SZBI w MS powodował, że wymogi określone w § 20 ust. 1 rozporządzenia KRI, zobowiązujące podmiot realizujący zadania publiczne do *wdrożenia, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniający jej poufność, dostępność i integralność* nie były spełnione.

Na powyższe zwracały również uwagę przeprowadzone w latach 2013–2014 audyty wewnętrzne. Pomimo tego realne działania na rzecz poprawy tego stanu rzeczy rozpoczęto dopiero w 2015 r.

Najwyższa Izba Kontroli stwierdziła, że opracowana w MS Polityka Ochrony Danych Osobowych np. nie zawierała wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych oraz opisu struktury danych wskazujących zawartość poszczególnych pól informacyjnych.

W MS sporządzono wprawdzie klasyfikację aktywów, niemniej jednak była ona niepełna i np. nie wymieniała m.in. kluczowych aktywów informacyjnych ministerstwa, niezbędnych do realizacji najważniejszych procesów instytucji, wraz ze wskazaniem poziomów ich ochrony.

Podobnie – klasyfikacja informacji była sporządzona nierzetelnie m.in. nie uwzględniała wszystkich informacji, nie wprowadzono pełnych zasad oznaczania informacji i postępowania z nimi. Ponadto nie wszystkie informacje, usługi, aplikacje miały przypisanych właścicieli, co powodowało, że nie została określona odpowiedzialność za poszczególne aktywa.

Zdaniem NIK na zapewnienie bezpieczeństwa systemów teleinformatycznych negatywny wpływ miały braki kadrowe oraz rotacja kadr w Departamencie Informatyzacji i Rejestrów Sądowych. W okresie objętym kontrolą (22 miesiące) kierowało Departamentem sześciu zastępców dyrektora, nieobsadzone pozostawały stanowiska dwóch naczelników wydziałów. W tym okresie na 120 pracowników departamentu odeszły z pracy 44 osoby (następne 4 na dzień 6 listopada były w okresie wypowiedzenia), co stanowiło 40 % obsady etatowej, a zatrudniono 22 osoby. Zdaniem NIK skutkiem braków kadrowych był m.in. fakt, że każdy administrator systemu administruje od 2 do 5 systemami, co stwarza ryzyko niewypełnienia wymogów określonych w § 20 ust. 2 pkt 12 rozporządzenia KRI zobowiązującego podmiot realizujący zadania publiczne do *zarządzania bezpieczeństwem informacji m.in. poprzez stworzenie warunków umożliwiających zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych*.

W MS brak było systemu zarządzania ryzykiem, w szczególności nie dokonywano okresowych analiz ryzyka i planów postępowania z ryzykiem, co naruszało § 20 ust. 2 pkt 3 rozporządzenia KRI, zgodnie z którym, *kierownictwo podmiotu publicznego realizuje zarządzanie bezpieczeństwem informacji poprzez zapewnienie warunków umożliwiających przeprowadzenie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy*.

Wdrożone w MS w lipcu 2015 r. zasady zarządzania incydentami odnosiły się wyłącznie do zasad ich dokumentowania, nie zawierały regulacji dot. zbierania związanych z nimi dowodów.

Ponadto prowadzona w MS ewidencja incydentów w okresie co najmniej do lipca 2015 r. nie zapewniała odpowiednich warunków dla analizowania przypadków naruszania bezpieczeństwa informacji, w celu doskonalenia systemu zabezpieczeń. Nie spełnione zostały zatem wymagania określone w § 20 ust. 2 pkt 13 rozporządzenia KRI dot. *zapewnienia warunków umożliwiających realizację i egzekwowanie obowiązku bezzwłocznego zgłaszania incydentów naruszania bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących*.

Dokumentacja polityki nie zawierała regulacji odnoszących się do zapobiegania złośliwemu oprogramowaniu, nie zawarto takich regulacji również w innych dokumentach.

Stosowane w MS zasady przetwarzania mobilnego oraz pracy na odległość nie zapewniały warunków pełnego bezpieczeństwa wykonywanych czynności, co nie spełniało wymagań określonych w § 20 ust. 2 pkt 8 rozporządzenia KRI.

W regulacjach wewnętrznych administratorzy systemów zobowiązani byli do analizowania logowań pod kątem kont nieużywanych przez ponad 30 dni. Pomimo tego, co najmniej do końca 2014 r. nie przeprowadzano przeglądu aktualności kont użytkowników.

3.3.4. Ministerstwo Skarbu Państwa

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości, **NIK oceniła poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów teleinformatycznych" w MSP jako *powtarzalny* lecz *intuicyjny***.

W kontrolowanej jednostce istniała świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak była ona fragmentaryczna i ograniczona. Wprawdzie rozwijano politykę dotyczącą bezpieczeństwa, ale nie towarzyszyły temu adekwatne narzędzia. Chociaż systemy dostarczały informacji dotyczących bezpieczeństwa, to dane te nie były analizowane.

Bezpieczeństwo IT było postrzegane głównie, jako przedmiot odpowiedzialności i domena działu IT, a nie zadanie leżące w gestii całego Ministerstwa.

W MSP nie została opracowana Polityka Bezpieczeństwa zgodnie z § 20 ust. 1 i § 15 ust. 2 rozporządzenia KRI. Funkcjonująca w Ministerstwie Polityka nie spełnia w ocenie NIK wymagań rozporządzenia, zawierała bowiem jedynie ogólne zasady bezpieczeństwa teleinformatycznego, bez szczegółowych procedur i nie mogła stanowić spójnego systemu ochrony informacji. Nie uregulowano m.in. kwestii: procedury dostępu do obszarów bezpiecznych, zarządzania dostępem do sieci LAN, rejestrowania i wyrejestrowywania użytkowników, rejestrowania konta użytkowania, jak również formalnie przyjętej polityki zapobiegania złośliwemu oprogramowaniu.

Podstawy formalne systemu zarządzania bezpieczeństwem informacji były w trakcie kontroli opracowywane w ramach budowy System Zarządzania Bezpieczeństwem Informacji, którą zlecono w dniu 3 listopada 2013 r. zewnętrznej firmie. Firma ta miała przeprowadzić audyt bezpieczeństwa infrastruktury sieciowej i wdrożyć SZBI. Przeprowadzony audyt potwierdził, że w Ministerstwie nie funkcjonuje SZBI oraz wydał zalecenia m.in. odnośnie kwerendy infrastruktury IT pod kątem aktualności stosowanego oprogramowania, wdrożenia polityki haseł i blokowania kont użytkowników. Do dnia zakończenia kontroli powyższe rekomendacje były w trakcie realizacji.

Brak było jednolitego zcentralizowanego rejestru incydentów, co w ocenie NIK, uniemożliwiało rzetelne monitorowanie stanu bezpieczeństwa jednostki. Ponadto nie zdefiniowano mierników pozwalających na identyfikację powtarzających się rodzajów incydentów i klasyfikację istotności. Brak jednolitej procedury reagowania na incydenty oraz jednoznacznego wskazania komórki odpowiedzialnej za reakcję, NIK oceniła jako nierzetelne i wskazujące na nieosiągnięcie wymogu określonego w § 20 ust. 2 pkt. 13 rozporządzenia KRI, zgodnie z którym *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących*.

Procesy związane z dystrybucją oprogramowania antywirusowego, jego aktualizacją oraz aktualizacją definicji dokonywane były automatycznie dla stacji roboczych w ramach domeny. Dla komputerów spoza domeny, instalacja oprogramowania wykonywana była przez pracowników IT, a proces aktualizacji oprogramowania, jak i definicji, konfigurowany był automatycznie. W toku kontroli nie przekazano dokumentacji potwierdzającej przeprowadzenie ww. weryfikacji oraz nie wskazano, w jaki sposób zapewniono aby wszystkie komputery spoza domeny posiadały zainstalowane oprogramowanie antywirusowe.

Prowadzona była ewidencja aktywów wspierających dotycząca infrastruktury sieciowej jednakże nie przypisano im poziomów ochrony.

Zapisy w dziennikach systemu (logach) nie spełniały wymagań, o których mowa w § 21 ust. 2 rozporządzenia KRI, zgodnie z którym *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:*

1) *systemu z uprawnieniami administracyjnymi,*
2) *konfiguracji systemu, w tym konfiguracji zabezpieczeń,*
3) *przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.*

Dzienniki systemowe prowadzone były w sposób nierzetelny i niezgodny z § 21 ust. 1 rozporządzenia KRI, zgodnie z którym *rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach)*. Powyższe potwierdziły nieprawidłowości wykryte w wyniku badania logów systemu – przykładowo stwierdzono ponad 1400 logowań, w których w miejscu nazwy użytkownika domeny pojawiało się puste pole.

3.3.5. Narodowy Fundusz Zdrowia

W oparciu o stosowany w metodyce COBIT 4.1 Model dojrzałości, **NIK oceniła poziom zarządzania procesem „zapewnienie bezpieczeństwa systemów informatycznych" w Centrali NFZ jako *powtarzalne* lecz *intuicyjne***.

W kontrolowanej jednostce istniała świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego, jednak była ona fragmentaryczna i ograniczona. Rozwijana była wprawdzie polityka dotycząca bezpieczeństwa, ale nie towarzyszyły jej adekwatne narzędzia. Chociaż systemy dostarczały informacji dotyczących bezpieczeństwa, dane te nie były analizowane.

W ocenie NIK brak jednolitego i kompleksowego systemu zarządzania bezpieczeństwem informacji w Centrali NFZ utrudniał właściwą ich ochronę. Nieaktualizowanie od 2010 r.[28] regulacji dotyczących bezpieczeństwa danych przetwarzanych w NFZ powodowało, że stosowane rozwiązania nie nadążały za zmianami w systemie prawnym, a w konsekwencji również mogły przyczyniać się do osłabienia tej ochrony. W tym kontekście Izba pozytywnie ocenia podjęte przez Fundusz działania w celu opracowania i wdrożenia[29] Zintegrowanego Systemu Zarządzania łączącego System Zarządzania Ryzykiem, System Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Ciągłością Działania.

W NFZ brak było całościowej polityki bezpieczeństwa informacji. Przyjęte zarządzenie z 2010 roku w sprawie bezpieczeństwa danych przetwarzanych w NFZ dotyczyło systemów przetwarzających dane osobowe. Regulacje te nie były aktualizowane, co stanowiło naruszenie wymogów określonych w § 20 ust. 2 pkt 1 rozporządzenia KRI. Zgodnie z tym przepisem *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia*. NIK, jako działanie nierzetelne oceniła fakt, że w Centrali NFZ brak było skutecznie działającego systemu zarządzania bezpieczeństwem informacji.

Przeprowadzony w 2013 r. audyt bezpieczeństwa systemu informacyjnego eWUŚ wskazał, że aplikacja ta była podatna na znane błędy bezpieczeństwa oraz ujawnił istnienie ryzyk w obszarze bezpieczeństwa informacji. Przeprowadzony po trzech miesiącach audyt sprawdzający wykazał, że nie usunięto 40% podatności a 32% usunięto częściowo.

W NFZ nie był prowadzony zcentralizowany rejestr incydentów, co zdaniem NIK uniemożliwiało kierownictwu stworzenie odpowiednich warunków do monitorowania stanu bezpieczeństwa jednostki. Procedury zawierające definicje incydentu, szczegółowe zasady zgłaszania rejestrowania i analizowania incydentów były w trakcie opracowywania. Brak jednolitej procedury reagowania na incydenty i jednoznacznego wskazania komórki odpowiedzialnej za reakcję, było zdaniem NIK

[28] Wprowadzone Zarządzeniem Nr 12/2010/POIN Prezesa NFZ z dnia 29 stycznia 2010 r. w sprawie bezpieczeństwa danych przetwarzanych w Narodowym Funduszu Zdrowia.

[29] Zgodnie z harmonogramem projektu wdrożenia ZSZ przeprowadzenie pełnego wdrożenia ZSZ planowane było do końca 2016 r.

działaniem nierzetelnym oraz stanowiącym naruszenie wymogu określonego w § 20 ust. 2 pkt 13 rozporządzenia KRI. W obszarze ochrony przed złośliwym oprogramowaniem NIK nie stwierdziła nieprawidłowości. Systemem ochrony przed złośliwym oprogramowaniem objęto komputery stacjonarne i przenośne. W NFZ nie prowadzono klasyfikacji aktywów, w związku z powyższym nie mają one przyporządkowanych parametrów istotności i poziomów ochrony.

W dziennikach systemu eWUŚ (logach), w okresie objętym kontrolą, ponad 180 razy pojawiał się użytkownik „root"[30]. W czasie trwania kontroli wdrażany był system uniemożliwiający korzystanie z tego konta, który zapewni, że zmiany konfiguracyjne będą wykonywane wyłącznie przez użytkowników imiennych. W ocenie NIK powyższa nieprawidłowość wskazuje na naruszenie § 21 ust. 1 rozporządzenia KRI zgodnie z którym *rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach)*.

W zakresie zarządzania kontami użytkowników stwierdzono, że obowiązujące w NFZ procedury zobowiązywały komórkę kadrową do comiesięcznego przekazywania informacji o długotrwałych absencjach pracowników. Jednakże stwierdzono działania niezgodne z powyższą regulacją. W okresie objętym kontrolą komórka kadrowa nie przekazała 13 takich informacji. Zaniechanie poinformowania działu IT o zmianach kadrowych niesie ze sobą ryzyko dostępu osób nieuprawnionych do zasobów Centrali NFZ.

W regulacjach wewnętrznych poza ogólnymi zapisami, że w NFZ przetwarzane są dane osobowe (w tym wrażliwe) oraz inne dane prawnie chronione, w szczególności: medyczne, finansowe i kadrowe nie uregulowano zasad postępowania z danymi innymi niż osobowe. W praktyce regulacje te określały przede wszystkim przetwarzanie danych osobowych, nie regulowały zaś szczegółowo informacji chronionych rozumianych jako, informacje nie podlegające obligatoryjnemu obowiązkowi ochrony, ale które powinny być chronione ze względu na dobrze pojęty interes NFZ, pracowników NFZ lub podmiotów i instytucji, z którymi NFZ współpracuje. W powyższej dokumentacji nie dokonano klasyfikacji informacji przetwarzanych w NFZ, w tym nie zidentyfikowano danych (nie sporządzono ewidencji informacji i danych), których ochrona nie jest prawnie wymagana, a mogłyby one zostać wykorzystane przeciwko NFZ poprzez ujawnienie, zablokowanie lub zmanipulowanie. W badanym okresie w NFZ formalnie nie określono zasad identyfikacji i oznaczania danych oraz informacji, w tym danych wrażliwych czy chronionych. Z wyjaśnień uzyskanych w trakcie kontroli wynika, że takie zasady były w trakcie opracowywania. NIK oceniła jako nierzetelne nieprzypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla Centrali NFZ.

3.3.6. Komenda Główna Straży Granicznej

W oparciu o stosowany w metodyce CobiT 4.1 Model dojrzałości, **NIK oceniła poziom zarządzania procesem zapewnienia bezpieczeństwa systemów teleinformatycznych w Komendzie Głównej Straży Granicznej jako *początkowy/doraźny***.

W jednostce tej dotychczas nie utworzono formalnych podstaw do zapewnienia bezpieczeństwa w szczególności rzetelnej polityki bezpieczeństwa IT. Komendant Główny Straży Granicznej nie wprowadził podstawowych uregulowań dotyczących zarządzania procesem bezpieczeństwa pomimo, że opracowanie takich procedur zalecali audytorzy wewnętrzni KGSG już w październiku

[30] Tradycyjna nazwa uniksowego konta, które ma pełną kontrolę nad systemem.

2013 r. NIK negatywnie oceniła dwuletnią zwłokę w realizacji zaleceń ww. audytu. W KGSG bezpieczeństwo IT nie podlegało pomiarowi ze względu na nieokreślenie mierników bezpieczeństwa informacji i zasad jego monitorowania.

Zapewnienie bezpieczeństwa oparte było głównie na powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych i informacji niejawnych. KGSG dopiero w II kwartale 2015 r. realnie rozpoczęła budowę formalnych podstaw systemu zapewnienia bezpieczeństwa informacji. Powyższe przedsięwzięcie realizowane było we współpracy z NASK (Naukową i Akademicką Siecią Komputerową). Zdaniem NIK wdrożenie tego systemu wymagało przeprowadzania rzetelnej analizy ryzyka utraty informacji (po uprzednim wprowadzeniu formalnych podstaw szacowania i postępowania z ryzykiem) oraz określenia i wdrożenia systemu monitorowania procesów związanych z bezpieczeństwem informacji.

W KGSG nie dokonano szczegółowej analizy przetwarzanych informacji wraz z przypisaniem im istotności dla funkcjonowania SG. Najważniejsze dla SG informacje były chronione na podstawie ustawy o ochronie informacji niejawnych.

Komendant Główny Straży Granicznej nie opracował i nie wdrożył metodologii procesu szacowania ryzyka bezpieczeństwa informacji oraz postępowania z tym ryzykiem, w tym systematycznego jego monitorowania i analizy.

Ustalono, że incydenty bezpieczeństwa dotyczące infrastruktury technicznej były gromadzone i analizowane. Jednakże w KGSG nie zbudowano formalnych podstaw systemu zbierania i analizy incydentów bezpieczeństwa, co stanowiło naruszenie § 20 ust. 2 pkt 13 rozporządzenia KRI, zgodnie z którym *kierownictwo zapewnia bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących*.

3.3.7. Ministerstwo Spraw Wewnętrznych

W oparciu o stosowany w metodyce COBIT 4.1 Model dojrzałości, **NIK oceniła poziom zarządzania bezpieczeństwem systemów teleinformatycznych jako *początkowy/doraźny*.**

MSW dostrzegało potrzebę zapewnienia bezpieczeństwa IT, jednakże było ono zapewniane na doraźnych zasadach, zależało głównie od pojedynczych osób i nie podlegało pomiarowi.

W MSW nie wprowadzono formalnych podstaw do Systemu Zarządzania Bezpieczeństwem Informacji, pomimo, że istniała w tej jednostce świadomość potrzeby zapewnienia bezpieczeństwa teleinformatycznego. W MSW bezpieczeństwo informacji nie podlegało pomiarowi. Nie uszeregowano hierarchicznych celów w zakresie bezpieczeństwa, pozwalających na osiągnięcie w określonym czasie oczekiwanych poziomów bezpieczeństwa informacji, nie przypisano im niezbędnych zasobów, nie opracowano również mierników. Nie powołano właściwej komórki odpowiedzialnej za zarządzanie bezpieczeństwem systemów teleinformatycznych, pomimo że wyniki przeprowadzonych audytów rekomendowały powołanie jednej komórki organizacyjnej w tym zakresie. Zagadnienia zawiązane z bezpieczeństwem IT były rozproszone pomiędzy kilka komórek, a w trakcie kontroli stwierdzono spory kompetencyjne pomiędzy tymi komórkami.

W MSW nie przeprowadzono procesu identyfikacji zasobów istotnych dla realizowanych zadań, nie przypisano im istotności i niezbędnych poziomów ochrony.

W MSW nie określono procedur reagowania na incydenty, a nawet nie wprowadzono jednoznacznej definicji incydentu bezpieczeństwa. Nie określono również komórki, która miałaby reagować

na incydenty, nie prowadzono również rejestru incydentów. Zarządzanie problemami odbywało się na zasadach doraźnych, czego przykładem może być fakt, że z 55 incydentów dotyczących MSW zarejestrowanych przez zespół CERT.GOV.PL w 8 przypadkach Ministerstwo nie było w stanie zidentyfikować żadnych szczegółów incydentu i podać sposobu reakcji. Powyższe, w ocenie NIK, stanowiło naruszenie wymogu określonego w § 20 ust. 1 rozporządzenia KRI, według którego *podmiot realizujący zadania publiczne opracowuje i ustanawia, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji*.

Polityka zapobiegania złośliwemu oprogramowaniu nie została w sposób formalny określona, co w ocenie Izby przyczyniło się do wystąpienia przypadków braku oprogramowania antywirusowego na stacjach roboczych pracowników MSW lub nieaktualność takiego oprogramowania. Logi z programów antywirusowych były przeglądane, jednakże obowiązek taki nie został sformalizowany.

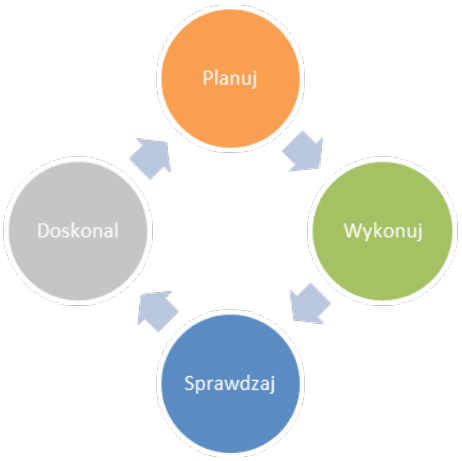
Brak było w MSW ewidencji aktywów wspierających, dotyczących infrastruktury sieciowej. NIK oceniła poziom zarządzania procesem bezpieczeństwa teleinformatycznego wybranego systemu – Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych jako „nieistniejący", tj. organizacja nie dostrzegała potrzeby zapewnienia bezpieczeństwa, zakładając że uzyskanie oczekiwanego poziomu bezpieczeństwa możliwe będzie dzięki całkowitej separacji sieci systemu od sieci publicznej. Tymczasem ABW stwierdziła przypadek korzystania przez użytkownika CEWiUDP ze stacji połączonej z siecią publiczną. MSW nie miało możliwości sprawdzenia tej separacji, m.in. nie posiadało możliwości automatycznego wykrywania przypadków braku separacji tych sieci. Nie sporządzano zapasowej, drugiej kopii danych CEWIUDP, a taśmy z kopiami danych nie były zabezpieczone kryptograficznie. Naruszono również przepis § 21 ust. 4 rozporządzenia KRI, zgodnie z którym *informacje w dziennikach systemów powinny być przechowywane przez minimum 2 lata,* gdy tymczasem były przechowywane przez 30 dni.

4 INFORMACJE DODATKOWE

4.1 Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Pomimo że nie istnieją rozwiązania gwarantujące stabilną i stuprocentową skuteczność ochrony informacji, jednakże **zapewnienie bezpieczeństwa informacji na zakładanym poziomie jest możliwe tylko poprzez systemową, ciągłą realizację odpowiednich procesów**.

Zdaniem NIK powinno się to odbywać według poniższego schematu przedstawiającego główne elementy systemu bezpieczeństwa informacji[31].



Źródło: Opracowanie własne NIK.

Ograniczone zasoby finansowe, kadrowe i czasowe, którymi dysponują podmioty publiczne nie pozwalają na uzyskanie idealnego stanu, w którym wszystkie te elementy uzyskałyby swój najwyższy poziom. Według NIK w badanym obszarze konieczna jest więc **ciągła analiza potrzeb i zagrożeń; metodyczne podejmowanie decyzji o wyborze najważniejszych w danym momencie celów; odpowiednie planowanie pozwalające na sukcesywne dążenie do ich osiągniecia, refleksja nad uzyskanymi efektami i powrót do rozpoczynającej kolejny cykl analizy**. Taki schemat postępowania daje szanse zarówno optymalnego dysponowania ograniczonymi zasobami, jak również elastyczne reagowanie na zmieniające się warunki.

W ramach przedmiotowej kontroli NIK objęła kontrolą wszystkie elementy systemu bezpieczeństwa informacji według schematu: planuj, wykonaj, sprawdzaj, doskonal zgodnie z powyższym schematem.

Poniższe diagramy przedstawiają główne obszary objęte kontrolą w ramach poszczególnych elementów systemu wraz z powiązaniami między nimi.

[31] Cykl Deminga (określany też jako cykl PDCA z ang. Plan-Do-Check-Act lub cykl P-D-S-A z ang. Plan-Do-Study-Act lub koło Deminga) – schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, Kaizen), stworzoną przez Williama Edwardsa Deminga, amerykańskiego specjalistę statystyka pracującego w Japonii.

Diagram nr 1

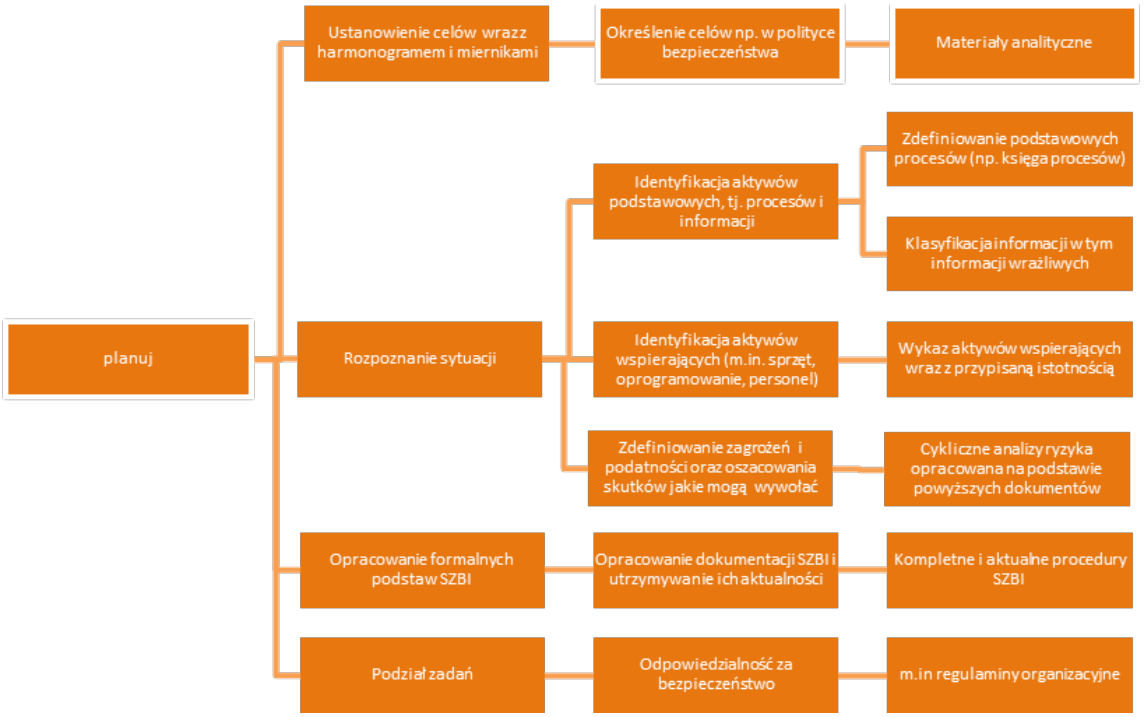


Diagram nr 2

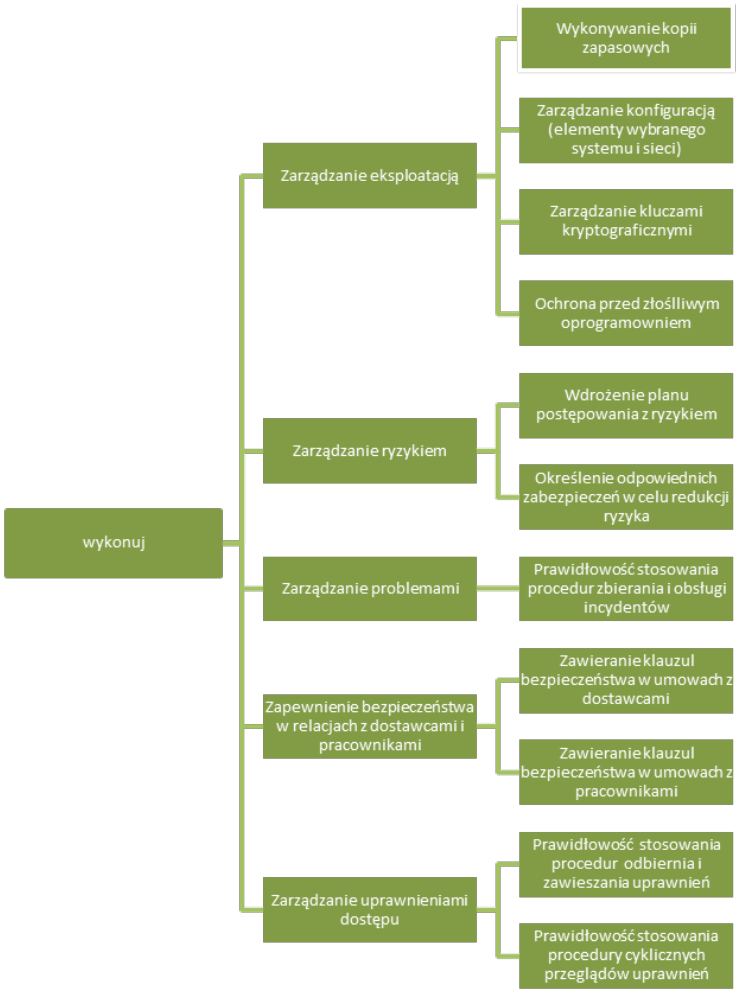


Diagram nr 3

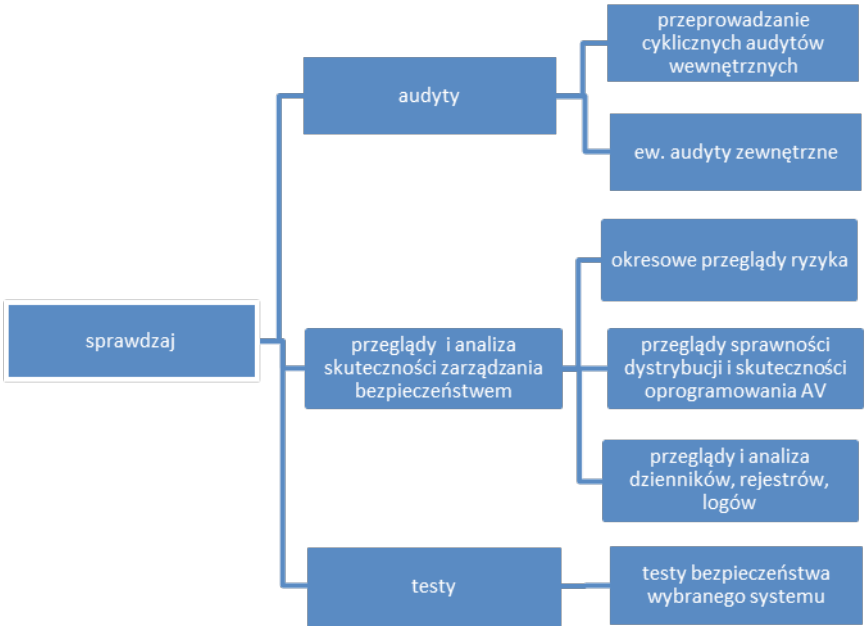
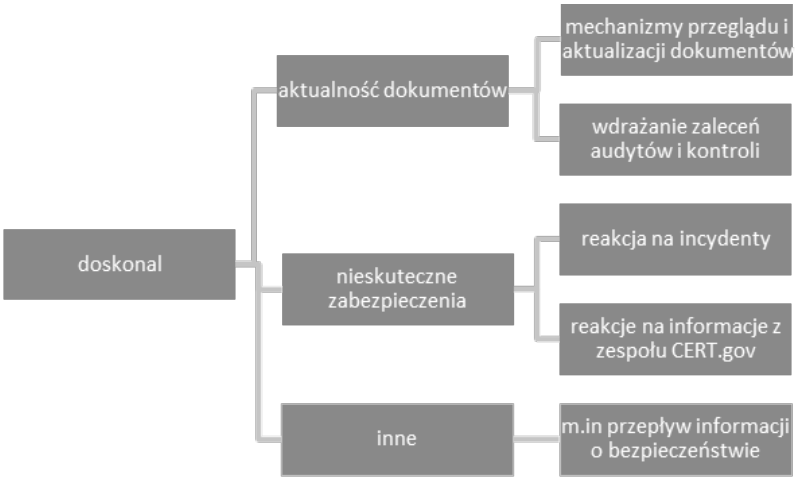


Diagram nr 4



Źródło: Opracowanie własne NIK.

Postępowania kontrolne zostały przeprowadzone w okresie od 1 czerwca 2015 r. do 28 grudnia 2015 r. W procesie opracowywania programu kontroli (zwłaszcza w części dot. metodyki działań), formułowania w wystąpieniach pokontrolnych ocen za pomocą metodyki COBIT oraz opracowania Informacji o wynikach kontroli NIK korzystała ze wsparcia eksperta z dziedziny objętej kontrolą.

Działając na podstawie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, kontrolerzy w trakcie kontroli w Ministerstwie Spraw Wewnętrznych uzyskali dodatkowe informacje od Szefa Agencji Bezpieczeństwa Wewnętrznego w sprawie informacji o incydentach związanych z naruszeniem bezpieczeństwa informacyjnego w kontrolowanych instytucjach, pozyskanych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.gov.pl. Zespół przekazał listę 267 incydentów bezpieczeństwa dotyczących jednostek kontrolowanych zarejestrowanych w okresie kontroli.

W 6 wystąpieniach pokontrolnych skierowanych do kierowników kontrolowanych jednostek sformułowano łącznie 19 wniosków pokontrolnych, zmierzających do wyeliminowania stwierdzonych nieprawidłowości, z tego 11 jest w trakcie realizacji, a 8 nie zostało zrealizowanych.

Do Ministra Sprawiedliwości NIK wniosła o:

- Uporządkowanie i uproszczenie struktury zarządzania bezpieczeństwem informacji w Ministerstwie Sprawiedliwości, na poziomie organizacyjnym oraz dokumentacji polityk bezpieczeństwa, w tym rozważenie powołania Pełnomocnika odpowiedzialnego za nadzorowanie bezpieczeństwa informacji, wyposażonego w zasoby finansowe i osobowe – grupę ludzi o różnych kompetencjach i zakresie wiedzy z obszaru bezpieczeństwa informacji.
- Dokończenie, zapoczątkowanego w 2015 r., procesu świadomego budowania systemu zarządzania bezpieczeństwem informacji opartego na identyfikacji aktywów, identyfikacji zagrożeń dla poszczególnych aktywów oraz szacowaniu ryzyka tak, aby przygotowana dokumentacja SZBI w pełni odpowiadała specyfice Ministerstwa Sprawiedliwości, działu IT i innych komórek organizacyjnych.
- Proceduralne i faktyczne rozdzielenie procesu zgłaszania, ewidencjonowania i reagowania na incydenty związane z bezpieczeństwem informacji od zdarzeń dotyczących pomocy użytkownikom w obsłudze stacji roboczych i innych urządzeń IT oraz wykorzystanie analizy tych incydentów do zarządzania bezpieczeństwem informacji w skali danego systemu i w skali całej instytucji.
- Zoptymalizowanie korzystania z ustaleń i zaleceń audytów w sferze bezpieczeństwa teleinformatycznego, w celu uniknięcia zastępowania audytami (w szczególności zewnętrznymi) rzeczywistych działań podejmowanych na rzecz doskonalenia systemu zarządzania bezpieczeństwem informacji.

Do Ministra Spraw Wewnętrznych NIK wniosła o:

- Wprowadzenie zmian w organizacji MSW, w celu powierzenia całości zadań z zakresu bezpieczeństwa IT i odpowiedzialności za ich realizowanie jednej komórce;
- Opracowanie i wdrożenie, zgodnego z powszechnie przyjętymi standardami, Systemu Zarządzania Bezpieczeństwem Informacji.

Do Ministra Skarbu Państwa NIK wniosła o:

- Kontynuowanie działań związanych z wdrożeniem w MSP Systemu Zarządzania Bezpieczeństwem Informacji, w szczególności w zakresie przyjęcia kompletnej i spójnej polityki bezpieczeństwa systemów informatycznych.
- Zapewnienie pełnej rozliczalności Zintegrowanego Systemu Zarządzania.
- Prowadzenie jednego kompletnego rejestru incydentów.

Do Prezesa KRUS NIK wniosła o:

- Przeprowadzenie kwerendy obowiązujących procedur zmierzającej do dalszego ich udoskonalenia, zwiększenia czytelności, integralności i kompletności.
- Podjęcie czynności zmierzających do wzmocnienia nadzoru nad realizacją umów w modelu outsourcingu w powiązaniu z rzetelną analizą ryzyka w tym obszarze.
- Wypracowanie rzetelnego narzędzia monitorowania bezpieczeństwa informacji poprzez uszczelnienie i ujednolicenie systemu gromadzenia informacji o incydentach bezpieczeństwa przy jednoczesnej modyfikacji miernika procesu zarządzania bezpieczeństwem informacji.

- Podjęcie skutecznych działań na rzecz systematycznego i rzetelnego przeprowadzania przeglądu adekwatności uprawnień.
- Kontynuowanie działań zmierzających do zbudowania pełnego wykazu aktywów wspierających.

Do Prezesa Narodowego Funduszu Zdrowia NIK wniosła o:

- Kontynuowanie działań związanych z wdrożeniem w NFZ Zintegrowanego Systemu Zarządzania, w szczególności w zakresie przyjęcia kompletnej i spójnej polityki bezpieczeństwa systemów informatycznych.
- Przekazywanie informacji o absencjach przekraczających 30 dni zgodnie z przyjętymi uregulowaniami wewnętrznymi.
- Zapewnienie pełnej rozliczalności systemów teleinformatycznych poprzez wyeliminowanie przypadków stosowania typowych lub domyślnych loginów administratora np. „root".

Do Komendanta Głównego Straży Granicznej NIK wniosła o:

- Opracowanie i wdrożenie, zgodnego z powszechnie przyjętymi standardami, Systemu Zarządzania Bezpieczeństwem Informacji uwzględniającego wprowadzenie mierników procesu zarządzania bezpieczeństwem.
- Opracowanie i wdrożenie procesu szacowania ryzyka w bezpieczeństwie informacji oraz procesu postępowania z tym ryzykiem.

Zastrzeżenia do wystąpienia pokontrolnego NIK zgłosił tylko Minister Sprawiedliwości.
Kolegium Najwyższej Izby Kontroli w dniu 17 lutego 2016 r. oddaliło te zastrzeżenia w całości.

Wykaz osób zajmujących w okresie objętym kontrolą stanowiska kierownicze w badanych jednostkach

Lp.	Osoby kierujące kontrolowaną działalnością		Okres sprawowania funkcji	
1.	Minister Sprawiedliwości	Marek Biernacki	6 maja 2013 r.	22 września 2014 r.
		Cezary Grabarczyk	22 września 2014 r.	30 kwietnia 2015 r.
		Ewa Kopacz	30 kwietnia 2015 r.	4 maja 2015 r.
		Borys Budka	4 maja 2015 r.	16 listopada 2015 r
2.	Minister Spraw Wewnętrznych	Barłomiej Sienkiewicz	25 lutego 2013 r.	1 stycznia 2014 r.
		Teresa Piotrowska	1 stycznia 2014 r.	16 listopada 2015 r.
3.	Minister Skarbu Państwa	Andrzej Czerwiński	16 czerwca 2015 r.	16 listopada 2015 r.
		Włodzimierz Karpiński	24 kwietnia 2013 r.	16 czerwca 2015 r.
4.	Prezes KRUS	Artur Brzóska	5 stycznia 2012 r.	8 grudnia 2015 r.
5.	Szef NFZ	Marcin Pakulski	23 grudnia 2013 r.	28 lutego 2014 r.
		Wiesława Anna Kłos	1 marca 2014 r.	2 czerwca 2014 r.
		Tadeusz Jędrzejczyk	3 czerwca 2014 r.	do chwili obecnej
6.	Komendant Główny SG	gen. dyw. SG Dominik Tracz	11 kwietnia 2012 r.	31 grudnia 2015 r.

Wykaz aktów prawnych dotyczących kontrolowanej działalności

- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114).
- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, ze zm.).
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, ze zm.).
- Ustawa z dnia 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników (Dz.U. z 2016 r. poz. 277).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz. 113); szczególnie § 20, 21 i 23.
- Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094); szczególnie rozdział 2.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024); szczególnie § 3, 4, 5, 6, 7 i załącznik.

Wykaz organów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów Rzeczypospolitej Polskiej
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Cyfryzacji
8. Minister Spraw Wewnętrznych i Administracji
9. Minister Skarbu Państwa
10. Minister Sprawiedliwości
11. Minister Koordynator Służb Specjalnych
12. Prezes Narodowego Funduszu Zdrowia
13. Prezes Kasy Rolniczego Ubezpieczenia Społecznego
14. Komendant Główny Straży Granicznej
15. Szef Agencji Bezpieczeństwa Wewnętrznego
16. Dyrektor Rządowego Centrum Bezpieczeństwa
17. Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
18. Sejmowa Komisja Administracji i Spraw Wewnętrznych
19. Sejmowa Komisja do Spraw Kontroli Państwowej
20. Senacka Komisja Praw Człowieka, Praworządności i Petycji
21. Senacka Komisja Samorządu Terytorialnego i Administracji Państwowej